SAP Security Interview Questions

By : Nagar

Q. SAP Security T-codes
Frequently used security T-codes

SU01 - Create/ Change User SU01 Create/ Change User
PFCG - Maintain Roles
SU10 - Mass Changes
SU01D - Display User
SUIM - Reports
ST01 - Trace
SU53 - Authorization analysis

Q How to create users?
Execute transaction SU01 and fill in all the field. When creating a new user, you must enter an initial password for that user on the Logon data tab. All other data is optional.

Q What is the difference between USOBX_C and USOBT_C?
The table USOBX_C defines which authorization checks are to be performed within a transaction and which not (despite authority- check command programmed). This table also determines which authorization checks are maintained in the Profile Generator.

The table USOBT_C defines for each transaction and for each authorization object which default values an authorization created from the authorization object should have in the Profile Generator.

Q What authorization are required to create and maintain user master records?
The following authorization objects are required to create and maintain user master records:

S_USER_GRP: User Master Maintenance: Assign user groups
S_USER_PRO: User Master Maintenance: Assign authorization profile
S_USER_AUT: User Master Maintenance: Create and maintain authorizations

Q List R/3 User Types
Dialog users are used for individual user. Check for expired/initial passwords. Possible to change your own password. Check for multiple dialog logon

A Service user - Only user administrators can change the password. No check for expired/initial passwords. Multiple logon permitted

System users are not capable of interaction and are used to perform certain system activities, such as background processing, ALE, Workflow, and so on.

A Reference user is, like a System user, a general, non-personally related, user. Additional authorizations can be assigned within the system using a reference user. A reference user for additional rights can be assigned for every user in the Roles tab.

Q What is a derived role?

Derived roles refer to roles that already exist. The derived roles inherit the menu structure and the functions included (transactions, reports, Web links, and so on) from the role referenced. A role can only inherit menus and functions if no transaction codes have been assigned to it before.

The higher-level role passes on its authorizations to the derived role as default values which can be changed afterwards.
Organizational level definitions are not passed on. They must be created anew in the inheriting role. User assignments are not passed on either.

Derived roles are an elegant way of maintaining roles that do not differ in their functionality (identical menus and identical
transactions) but have different characteristics with regard to the organizational level. Follow this link for more info

Q What is a composite role?
A composite role is a container which can collect several different roles. For reasons of clarity, it does not make sense and is
therefore not allowed to add composite roles to composite roles. Composite roles are also called roles.

Composite roles do not contain authorization data. If you want to change the authorizations (that are represented by a composite role), you must maintain the data for each role of the composite role.

Creating composite roles makes sense if some of your employees need authorizations from several roles. Instead of adding each user separately to each role required, you can set up a composite role and assign the users to that group.
The users assigned to a composite role are automatically assigned to the corresponding (elementary) roles during comparison.

Q What does user compare do?
If you are also using the role to generate authorization profiles, then you should note that the generated profile is not entered in the user master record until the user master records have been compared. You can automate this by scheduling report
FCG_TIME_DEPENDENCY on a daily.

SU24 Concept

- SAP Security- Authorizition

•Transaction **SU24** maintains the USOBT_C and USOBX_C tables. These tables hold the relationships between the particular transaction and its authorization objects. It is possible to add or subtract the checks performed in the transaction by changing the appropriate flag.

•The benefit of transaction SU24 occurs when transactions are added to or deleted from Role Groups using the Profile Generator.

•When new transactions are added, the Profile Generator will add all authorization values maintained in SU24 for the transaction(s).

•When deleting transaction the Profile Generator will remove all authorization values that are maintained in SU24 for the transaction.

•Activities performed:

•Check/Maintain Authorization Values

•Addition of Authorization Object to tcode

•Deletion of Authorization Object from tcode

Check Ind.	**Proposal**	**Meaning**	**Explanation**
Check	YS	Check /Maintained	The object will be inserted along with the values in the role. The object will be checked along with the values during runtime of the transaction.
Check	NO	Check	This object will not be inserted into the roles. A check on the object along with the values will be done during the runtime of the transaction
Do not Check	NO	Do Not Check	The object will not be inserted into the roles and there will not be any check performed during runtime of the transaction

Status Texts for authorizations

•**Standard:** All field values in the subordinate levels of the hierarchy are unchanged from the SAP defaults

•**Maintained:** At least one field in the subordinate levels of the hierarchy was empty by default and has since been filled with a value

•**Changed:** The proposed value for at least one field in the subordinate levels of the hierarchy has been changed from the SAP default value.

•**Manual:** You maintained at least one authorization in the subordinate hierarchy levels manually (it was not proposed by the Profile Generator).

Effect of SU24 changes in Role Groups

•Authorization objects are maintained in SU24 for a particular transaction code. When a transaction code is added to role, only the authorization objects having **check** as check indicator value and **yes** as proposal value, maintained for that tcode will be added into the role group.

•

1) Adding Tcodes to a role

When a new Tcode is added to a role

•When a new tcode is added to a role, going in either *change authorization data* or *expert mode* provides the same result. All the authorizations maintained for the tcode at SU24 level is added to the role.

•The program adds new standard authorizations for objects in the roles If the authorization default values contain objects that

were previously not existing

Or only had authorizations in the status *Changed* or *Manual*

•A new standard authorization is not included

if the authorization fields contain identical authorizations in the status *Standard* in both authorizations, and the fields maintained in the old authorizations are empty in the new standard authorization.

If there were already authorizations in the status *Maintained* (active or inactive) or *Inactive Standard* before the merge, the program compares the values and the maintenance status of all authorization fields to determine whether new standard authorizations must be extended.

Changing SU24 values for a tcode

If the authorization data is changed for any tcode in SU24 and tcode is already present in the role, then going in the expert mode with option "*read old data and compare with new data*" will only reflect the additional changes. *Change authorization data* will not pull the new data for the tcode maintained at SU24 level

2) Removing Tcodes from the role

When you remove transactions from the role menu, this has the following effect on the authorizations.

•A standard authorization for which the associated transaction was removed from the role menu is removed during the merge, unless at least one other transaction that remains in the menu uses the same authorization default value. This applies both for active and inactive standard authorizations.

•Authorizations in the statuses *Changed* and *Manual* are not affected by the merge. They are therefore always retained.

SU25 – Upgrade Tool for Profile Generator

- Important!!!,
- SAP Security Interview questions,
- SAP Security- Authorizition

Why SU25 is required?

- After upgrading SAP with the new release, you need to make adjustment to the all the roles and transaction codes**.SU25** is the transaction code for upgrading profile generator.
- This has 6 different steps and the execution of these steps depends on whether you were already using profile generator in the last release.

This transaction has 6 steps. This transaction is used to fill the customer tables of the Profile Generator the first time the Profile Generator is used, or update the customer tables after an upgrade. The customers tables of the Profile Generator are used to add a copy of the SAP default values for the check indicators and field values. These check indicators and field values are maintained in transaction SU24. If you have made changes to check indicators, you can compare these with the SAP default values and adjust your check indicators as needed.

Step1: If you have not yet used the Profile Generator or you want to add all SAP default values again, use the initial fill procedure for the customer tables.

If you have used the Profile Generator in an earlier Release and want to compare the data with the new SAP defaults after an upgrade, use steps 2a to 2d. Execute the steps in the order specified here.

-Step 2a: is used to prepare the comparison and must be executed first.

-Step 2b - If you have made changes to check indicators or field values in transaction SU24, you can compare these with the new SAP default values. The values delivered by SAP are displayed next to the values you have chosen so that you can adjust them if necessary. If you double-click on the line, you can assign check indicators and field values. You maintain these as described in the documentation for transaction SU24.

Note on the list of transactions to be checked To the right of the list you can see the status which shows
whether or not a transaction has already been checked. At first the status is set to to be checked. If you choose the transaction in the change mode and then choose save, the status is automatically set to checked.
By choosing the relevant menu option in the list of transactions you can manually set the status to checked without changing check indicators or field values, or even reset this status to to be checked.
If you want to use the SAP default values for all the transactions that you have not yet checked manually, you can choose the menu option to copy the remaining SAP default values.

-Step 2c: You can determine which roles are affected by changes to authorization data. The corresponding authorization profiles need to be edited and regenerated. The affected roles are assigned the status “profile comparison required”.

Alternatively you can dispense with editing the roles and manually assign the users the profile SAP_NEW (make sure the profile SAP_NEW only contains the subprofiles corresponding to your release upgrade. This profile contains authorizations for all new checks in existing transactions). The roles are assigned the status "profile comparison required" and can be modified at the next required change (for example, when the role menu is changed). This procedure is useful if a large number of roles are used as it allows you to modify each role as you have time.

-Step 2d: Transactions in the R/3 System are occasionally replaced by one or more other transactions.

This step is used to create a list of all roles that contain transactions replaced by one or more other transactions.

The list includes the old and new transaction codes. You can replace the transactions in the roles as needed. Double-click the list to go to the role.

Step 3: This step transports the changes made in steps 1, 2a, and 2b.

Tailoring the Authorization Checks
This area is used to make changes to the authorization checks.

Changes to the check indicators are made in **step 4**. You can also go to **step 4** by calling transaction SU24.

-You can then change an authorization check within a transaction.
-When a profile to grant the user authorization to execute a transaction is generated, the authorizations are only added to the Profile Generator when the check indicator is set to Check/Maintain.
-If the check indicator is set to do not check, the system does not check the authorization object of the relevant transaction.
-You can also edit authorization templates that can be added to the authorizations for a role in the Profile Generator. These are used to combine general authorizations that many users need. SAP delivers a number of templates that you can add directly to the role, or copy and then create your own templates, which you can also add to roles.

In **step 5** you can deactivate authorization objects systemwide.

In **step 6** you can create roles from authorization profiles that you generated manually. You then need to tailor and check these roles.

User Buffer

- SAP Security Interview questions,
- SAP Security- Authorizition

When a user logs on to the SAP R/3 System, a user buffer is built containing all authorizations for that user. Each user has their own individual user buffer. For example, if user Smith logs on to the system, his user buffer contains all authorizations of role USER_SMITH_ROLE. The user buffer can be displayed in transaction SU56.

A user would fail an authorization check if:

- The authorization object does not exist in the user buffer
- The values checked by the application are not assigned to the authorization object in the user buffer
- The user buffer contains too many entries and has overflowed. The number of entries in the user buffer can be controlled using the system profile parameter **auth/number_in_userbuffer**.

What is the difference between USOBX_C and USOBT_C?

- SAP Security- Authorizition,
- Tac n Ticks

The table USOBX_C defines which authorization checks are to be performed within a transaction and which not (despite *authority-check* command programmed). This table also determines which authorization checks are maintained in the Profile Generator.

The table USOBT_C defines for each transaction and for each authorization object which default values an authorization created from the authorization object should have in the Profile Generator.

What authorization are required to create and maintain user master records?

- SAP Security Interview questions,
- SAP Security- Authorizition

The following authorization objects are required to create and maintain user master records:

- S_USER_GRP: User Master Maintenance: Assign user groups
- S_USER_PRO: User Master Maintenance: Assign authorization profile
- *S_USER_AUT*: User Master Maintenance: Create and maintain authorizations

Segregation of duties (SOD)

- Important!!!,
- SAP Security- Authorizition

Segregation of duties is a basic, key internal control and one of the most difficult to achieve. It is used to ensure that errors or irregularities are prevented or detected on a timely basis by employees in the normal course of business. Segregation of duties provides two benefits:

1) a deliberate fraud is more difficult because it requires collusion of two or more persons, and

2) it is much more likely that innocent errors will be found.

At the most basic level, it means that no single individual should have control over two or more phases of a transaction or operation. Management should assign responsibilities to ensure a crosscheck of duties.

- Authorizing a transaction, receiving and maintaining custody of the asset that resulted from the transaction.
- Receiving checks (payment on account) and approving write-offs.
- Depositing cash and reconciling bank statements.
- Approving time cards and having custody of pay checks.
- Having unlimited access to assets, accounting records and computer terminals and programs. For instance having access and using checks as the source documents to post to accounting records rather than using a check log or receipts.

There are four general categories of duties or responsibilities which are examined when segregation of duties are discussed: **authorization**, **custody**, **record keeping** and **reconciliation**.

In an ideal system, different employees would perform each of these four major functions. In other words, no one person should have control of two or more of these responsibilities. The more negotiable the asset, the greater the need for proper segregation of duties – especially when dealing with cash, negotiable checks and inventories. In those instances where duties cannot be fully segregated, mitigating or compensating controls must be established. Mitigating or compensating controls are additional procedures designed to reduce the risk of errors or irregularities. For instance, if the record keeper also performs a reconciliation process a detailed review of the reconciliation could be performed and documented by a supervisor to provide additional control over the assignment of incompatible functions. Segregation of duties is more difficult to achieve in a centralized, computerized environment. Compensating controls in that arena include passwords, inquiry only access, logs, dual authorization requirements, and documented reviews of input/output. Some special aspects of segregation of duties apply to IT functions themselves. There should be segregation between systems development and operations, operations and data control, and data base administration and system development.

SAP System Parameters

- Important!!!,
- SAP Security- Authorizition

This overview describes how security and controls can be implemented through system parameters. System parameters are used to maintain configuration over the operation of the SAP system. System parameters may define key settings for the whole system on which SAP runs, individual hosts systems (e.g. configuration for only one of many application servers) or the instances that are running on these servers. The majority of system parameters ensure that SAP operates effectively on the customer's preferred hardware, operating system and database platforms. System parameters also control how SAP operates and provides system wide control over some aspects of Security. System parameters are set using transaction RZ10. To make the parameters globally effective set them in the default profile, DEFAULT.PFL. To make them instance-specific, you must set them in the profiles of each application server in your R/3 System. System parameters can be reviewed with transaction TU02 or from the standard SAP report RSPARAM using transaction SA38.

Incorrect Logon, Default Clients and Default Start Menus

• Login/fails_to_session_end (default value – 3)

defines the number of times a user can enter an incorrect password before the system terminates the logon attempt.
• Login/fails_to_user_lock (default value – 12)
the number of times a user can enter an incorrect password before the system locks the user. If the system locks, an entry is written to the system log, and the lock is released at midnight.
• Login/failed_user_auto_unlock (default value – 1)
unlocks users who are locked by logging on incorrectly. The locks remain if the parameter value is 0.
• Login/system_client
This parameter specifies the default client. This client is automatically filled in on the system logon screen. Users can enter a different client.
• Login/ext_security
Since release 3.0E, external security tools such as Kerberos or Secude have managed R/3 System access. If this parameter is set, an additional identification can be specified for each user (in user maintenance) where users log on to their security system. To activate, set the value to X.
• rdisp/gui_auto_logout (default value – 0)
Maximum time allowed between input from the GUI before the frontend is automatically logged out. The value is set in seconds and the value of zero is used when this facility is not active.
• Start_menu
This parameter specifies the default start menu for all users and can be overwritten with the user-specific start menu (transaction SU50). The default is S000, and this value can be set to any other area menu code.

Password Security

System profile parameters define the minimum length of a password and the frequency with which users must change passwords.

• Login/min_password_lng
minimum password length. The minimum is three characters and the maximum eight characters.

• Login/password_expiration_time
number of days after which a password must be changed. The parameter allows users to keep their passwords without time limit and leaves the value set to the default, 0.
• To prevent use of a certain password, enter it in table USR40. Maintain this table with transaction SM30. In USR40, you may also generically specify prohibited passwords.
There are two wild-card characters:
– ? means a single character
– * means a sequence of any combination characters of any length
Examples:
– 123* in table USR40 prohibits any password that begins with the sequence 123.
– *123* prohibits any password that contains the sequence 123.
– AB? prohibits passwords that begin with AB and have an additional character, such as ABA, ABB, and ABC.

Securing SAP* user master record

• login/no_automatic_user_sapstar
By default SAP is installed with a user master record SAP*. This user has the profile SAP_ALL with access to all transactions and programs in SAP. By default if this user master record is deleted then SAP allows logon using SAP* and a password of 'PASS'. Although the user master record does not exist, SAP grants unrestricted system access privileges to SAP*. By setting this

parameter value to '1' this 'backdoor' access is blocked in the event the SAP* user master record is deleted. Prior to version 4.0 this parameter was login/no_automatic_user_sap*.

Tracing Authorizations

• Auth/check_value_write_on (default value – 0)
Authorization failures can be evaluated immediately they occur by running transaction SU53. This functionality is only active if the parameter is set to a value greater than zero in the system profile parameter.
• Auth/authorization_trace (version 4.0B onwards – default value – 'N')
When the parameter is set, any authorization checks performed are validated against existing entries in table USOBX. If the table does not contain the transaction/authorization object combination, then a new entry is added to the SAP reference table (i.e. USOBT not USOBT_C). Due to significant performance issues, SAP does not recommend this parameter being set in customer systems.
• Auth/test_mode (version 4.0B onwards – default value 'N')
When activated every authority check starts report RSUSR400. However SAP recommends not activating this parameter as the system is paralyzed if syntax errors occur in running the report and it has a significant performance impact .

Authority Check De-activation

• Auth/no_check_on_sucode (version 3.0E to version 3.1H – default value 'N'),
Auth/no_check_on_tcode (version 4.0 onwards – default value – 'N')
From release 3.0E, the system checks on object S_TCODE. In upgrades from versions prior to 3.0E to set this flag to 'Y' to ensure that old profiles operate in the new system. By default, the function is inactive.
The flag should not normally be switched on because of the degradation in security that results.

• Auth/no_check_in_some_cases (version 3.0F onwards -default value depends on release)
This parameter needs to be set to 'Y' for installation of the profile generator. It defines the use of table USOBT in the authority checks undertaken and allows authority checks to be disabled in individual transactions. Whilst SAP recommends switching off unnecessary authority checks, the full impact of this should be considered carefully.
• Auth/object_disabling_active (default value -'N')
Whilst_no_check_in_some_cases allows authority checks to be switched off in for individual transactions, this parameter allows checks on individual objects to be switched off globally within SAP. It is recommended that this parameter is not set.

Number of Authorizations in User Buffers

• Auth/auth_number_in_userbuffer
When a user logs onto SAP, the authorizations contained in the user's profiles are copied to a user buffer in memory. The maximum number of authorizations copied is set by this parameter. The size of the buffer must always exceed the maximum number of authorizations as authorization checks are made only against those in the buffer.

The default value is 800, but this can be set to between 1–2000. Refer to OSS notes 84209 and 75908 for more detailed information regarding changes to the size of the user buffer.
Transaction SU56 shows the contents of the user's user buffer and a total for all the authorizations in a user master record.

Table, ABAP and RFC system parameters

• Rec/client (default value – 'N')
The parameter switches automatic table logging on. Images of the table before and after are logged rather than just changes and so consideration to which tables are to be logged and log volumes must be made before using this as part of a control solution.

• Auth/rfc_authority_check (default value – '1')
The parameter determines how object S_RFC is checked during RFC calls. The object has three fields, activity, the name of the function being called and the function group in which the function resides. The parameter defines whether S_RFC object is checked and if so, whether the function group field is included in the validation.
Value = 0, no check against S_RFC
Value = 1, check active but no check for SRFC-FUGR
Value = 2, check active and check against SRFC-FUGR

• Auth/system_access_check_off (default value – '0' – check remains active)
This parameter inactivates the automatic authorization check for particular ABAP/4 language elements (file operations, CPIC calls, and calls to kernel functions). This parameter ensures the downward compatibility of the R/3 kernel.

Derive and Composite Role In SAP

- SAP Security- Authorizition,
- Tac n Ticks

Derived Role

- Derived roles refer to roles that already exist. The derived roles inherit the menu structure and the functions included (transactions, reports, Web links, and so on) from the role referenced. A role can only inherit menus and functions if no transaction codes have been assigned to it before.
- The higher-level role passes on its authorizations to the derived role as default values which can be changed afterwards. Organizational level definitions are not passed on. They must be created anew in the inheriting role. User assignments are not passed on either.
- Derived roles are an elegant way of maintaining roles that do not differ in their functionality (identical menus and identical transactions) but have different characteristics with regard to the organizational level.

Composite Role

- A composite role is a container which can collect several different roles. For reasons of clarity, it does not make sense and is therefore not allowed to add composite roles to composite roles. Composite roles are also called roles.
- Composite roles do not contain authorization data. If you want to change the authorizations (that are represented by a composite role), you must maintain the data for each role of the composite role.
- Creating composite roles makes sense if some of your employees need authorizations from several roles. Instead of adding each user separately to each role required, you can set up a composite role and assign the users to that group.

- The users assigned to a composite role are automatically assigned to the corresponding (elementary) roles during comparison.

Find the list of Transactions accesed by a particular user in a particular time period

- SAP Security Interview questions,
- Tac n Ticks

Goto ST03N->Expert mode–>Total–>Month–>User and Settlement Statistics–>User Profile–> Find….you will get your desire result.

You can also use use STAD, STAT, STATTRACE, SLG1

What is 'PFCG_TIME_DEPENDENCY'?

- SAP Security Interview questions,
- Tac n Ticks

Its like PFUD (Comparing User Master Records). If report 'PFCG_TIME_DEPENDENCY' is run the authorization profiles in the user master will be current.

Its better to run as background Job. Report PFCG_TIME_DEPENDENCY must also have run after each import of activity groups from other systems.

When to use SU24?

- Important!!!,
- SAP Security Interview questions,
- SAP Security- Authorizition

- To correct authorization objects that are not linked to transaction codes correctly

- To correct authorization objects that have unacceptable default values.

- To change default values to ones that will always be appropriate for all roles that will ever use the transaction. This means having blank fields where you need to allow different roles to have different values.

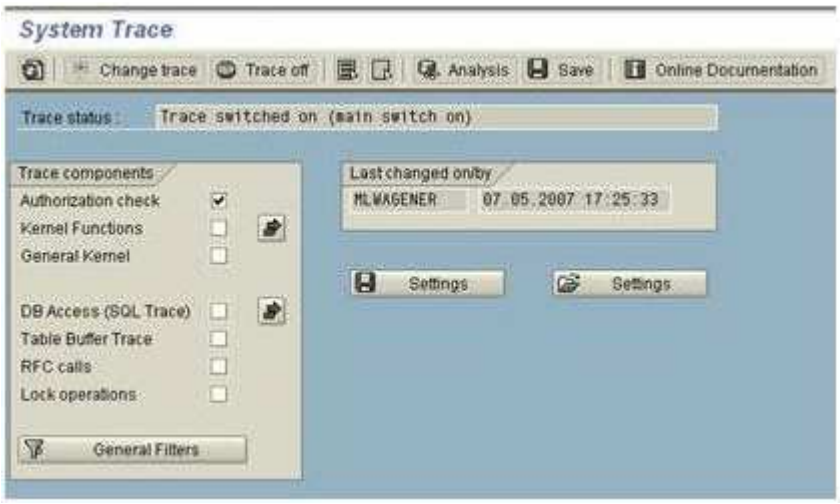
The system trace (ST01)

- Important!!!,
- SAP Security- Authorizition,
- Tac n Ticks

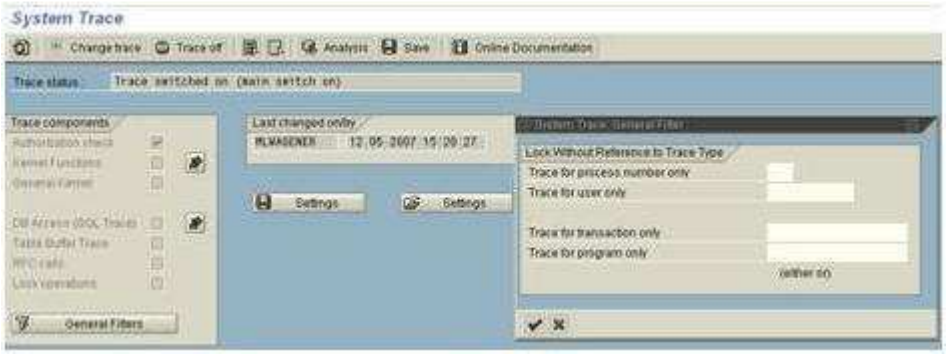
SAP offers with the system trace the opportunity to evaluate the authorization objects that are checked during the call of the different transactions. With the help of the trace all authorization objects, on which an authority check is executed while working with the system, can be logged.

This also includes the corresponding field values within the authorization objects.

Call the transaction **ST01** for the use of the system trace.



In the selection screen the different components can be activated via checkmark.

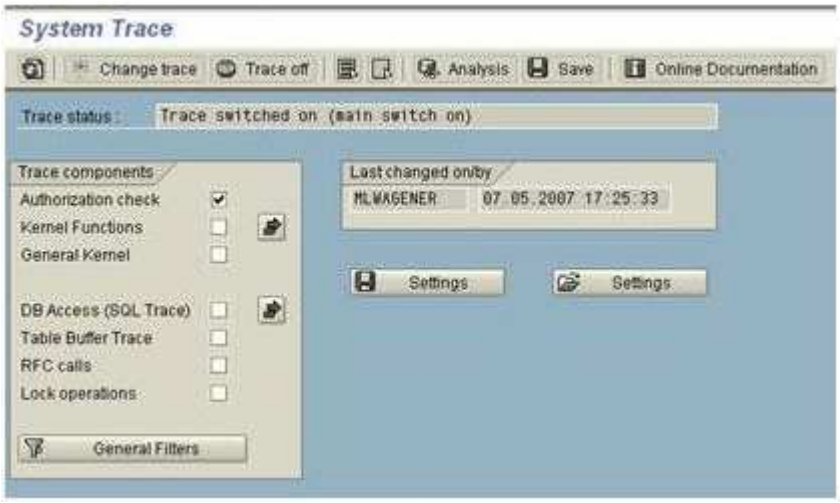


There are options for additional filter settings. Push the button *General Filters*. You can filter for the process you want to log, the user, the transaction, or the program.

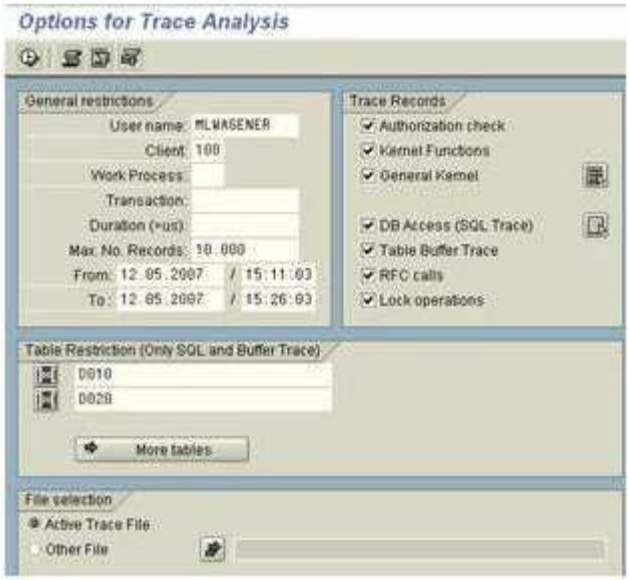
Enter the required selection, push the *key Enter*, and then activate the trace.

Note: An activation of the trace for all system users should not be activated. For user evaluation always enter the username you want to analyze. With activation of the trace all required access rights for the selected user will be logged. When all actions are traced, and logged, then please switch the *Trace off*.

After that you can evaluate the results by pushing the button ***Analysis*** [or key F2]. The evaluation path varies in dependency of the current release level.



Activate the integrated button *Analysis*. Enter the required selection for evaluation, and push the key *F8* for activation.



Trace in a multiple instance environment

In case you run SAP® on different instances you have to make sure that you activate the trace for the instance on which the user is executing the transactions that need to be logged for evaluation. Users can be active on more than one instance. [The user instance information is displayed down on the right in the SAP status bar.] You can review, and even change to the corresponding instance, with the help of transaction **SM51**. Select the instance you want to review. Activate the button *User Info* [CTRL+SHIFT+F7]. Select the user from the correspond list.
Mark the entry. In the menu bar select the path *Goto – Terminals.*
Select the user. In the menu bar select the path *Goto – Remote Server.*
From here you can activate the trace for the instance on which the user is located.

The trace evaluation

For interpretation of the evaluation you can use the following overview of relevant information.

Element	Info	Additional info
Time	Exact milli second.	Per double-click onto the selected entry you branch to the detail view.
Type	Type of the corresponding trace entry	Display of the selected trace component. See component overview
Duration	Duration of the trace	Not useful for authorization trace
Object	Objekt in dependency of the related component	See: component overview
Trace-message text		Per double-click onto the selected entry, you branch into the detail view. From there, you can branch into the related ABAP source code.

Please find the component overview with corresponding acronyms.

Component	Acronym	Object
Authorization check	AUTH	Authorization object t
Kernel-Functionen	CMOD	Related C- function in kernel
Kernel general	USER	C-Modul im Kernel, in dem der Trace geschrieben wird
DB-access (SQL-Trace)	SQL	DB-Table that was accessed
Table buffer-Trace	BUFF	DB- that was accessed
RFC-call	RFC	Called function module
Lock operation	ENQUE	Lock object

The return code

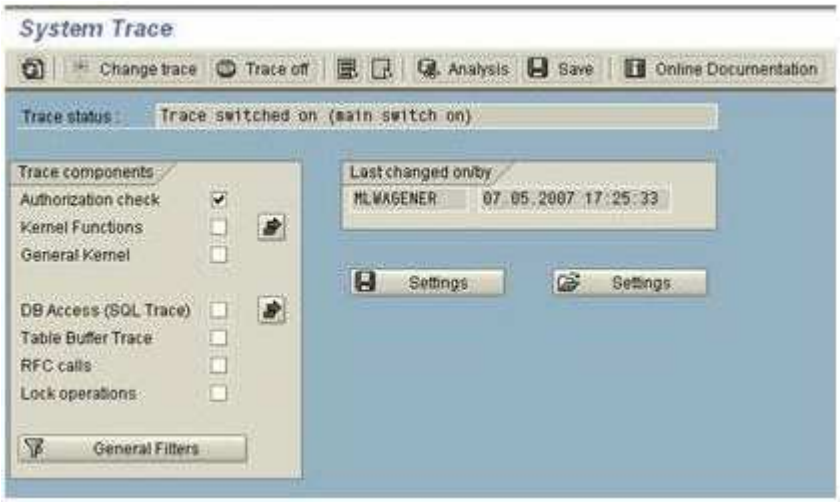
Successfully passed authorization check are marked in dark green already and have the value RC=0 added in the column next to the authorization object.

RC is the acronym for return code.

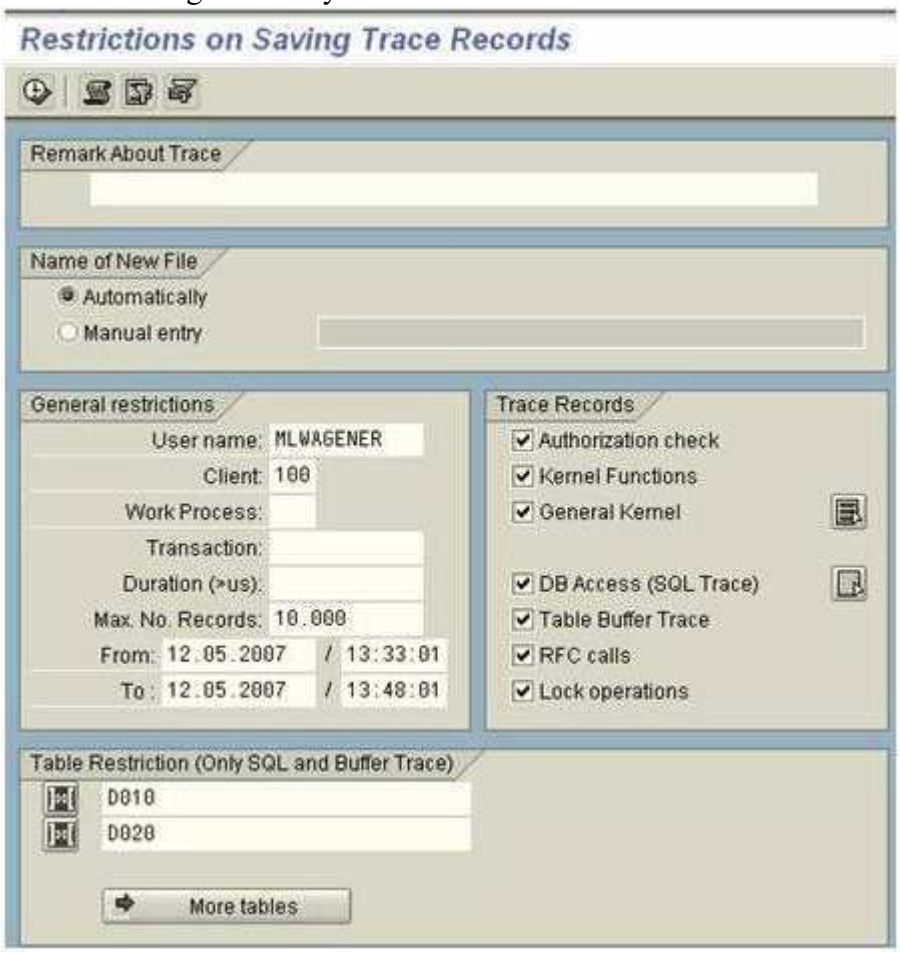
The return values vary depending on the check result. For example:
The return code *0* means that the authorization was successfully checked.
The return code *4* says, that the required authorization for the authorization object in the user master is not available.
The return code *12* says, that no authorization for the authorization object is available.

Saving of trace results

There are different ways to save trace evaluation results.
You can download the trace file in the evaluation display mode by saving the list locally.
If trace information are to be protected against overwriting,
you have to branch to the button *Save* after tracing.



In the following window you can enter remarks as well as a file name.



If you do not enter an absolute path when entering the file name manually, the file will be created in the log directory.
For the automatic file name creation, the system provides a file name, and creates the file in the log directory.
Automatically created file names can be selected with the *F4* search key in the future. This option is not available for manually created names.
Automatically created file names can be deleted within this application, manually created file names need to be deleted on the OS level separately.
Therefore the automatic file name creation is to be preferred.

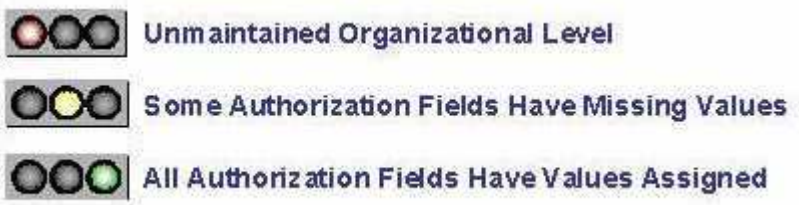
The system trace cannot only be used for the evaluation of authority checks, but also for evaluation of kernel functions, kernel modules, DB access, table buffer, RFC calls and lock operations. For system monitoring the developer trace is usually preferred.

SAP Security T-codes

- Important!!!

- SU01 Create/ Change User SU01 Create/ Change User
- PFCG Maintain Roles
- SU10 Mass Changes
- SU01D Display User
- SUIM Reports
- ST01 Trace
- SU53 Authorization analysis
- SE16 View Table or view.
- SM 30,31 , view and maintain table or view.
- SE93. Find prog link to the TCode
- su56 User Buffer.
- SM59 RFC maintain
- SM36 Schedule Background Job
- SM37 Overview of job selection
- SM01 Lock Transactions
- SM02 System Messages
- SM04 User List
- SM12 Display and Delete Locks
- RZ10 Maintain Profile Parameters
- RZ11 Profile Parameter Maintenance
- SM19 Security A udit Configuration
- SM20 Security Audit Log Assessment
- SE10 Transport Organizer
- STMS Transport Management System
- AL08 Users Logged On

What does the different color light mean in profile generator?



Type of user in SAP

- Important!!!,

- SAP Security Interview questions,
- Tac n Ticks

The SAP system categorizes users into several types for different purposes as shown in the table below:

User Types

Type	Purpose
Dialog	Individual, interactive system access.
System	Background processing and communication within a system (such as RFC users for ALE, Workflow, TMS, and CUA).
Communication	Dialog-free communication for external RFC calls.
Service	Dialog user available to a larger, anonymous group of users.
Reference	General, non-person related users that allows the assignment of additional identical authorizations, such as for Internet users created with transaction SU01. No logon is possible.

Dialog (A)

- User type for exactly one interactive user (all logon types including Internet users):
- During a dialog log on, the system checks whether the password has expired or is initial. The user can change his or her password himself or herself.
- Multiple dialog logons are checked and, where appropriate, logged.

System (B)

- User type for background processing and communication within a system (internal RFC calls).
- A dialog logon is not possible.
- The system does not check whether the password has expired or is initial.
- Due to a lack of interaction, no request for a change of password occurs. (Only the user administrator can change the password.)
- Multiple logons are permissible.

Communication (C)

- User type for dialog-free communication between systems (such as RFC users for ALE, Workflow, TMS, and CUA):
- A dialog logon is not possible.
- Whether the system checks for expired or initial passwords depends on the logon method (interactive or not interactive). Due to a lack of interaction, no request for a change of password occurs.

Service (S)

- User type that is a dialog user available to a larger, anonymous group of users. Assign only very restricted authorizations for this user type:
- During a log on, the system does not check whether the password has expired or is initial. Only the user administrator can change the password (transaction SU01, Goto ® Change Password).
- Multiple logons are permissible.
- Service users are used, for example, for anonymous system accesses through an ITS service. After an individual authentication, an anonymous session begun with a service user can be continued as a person-related session with a dialog user.

Reference (L)

- User type for general, non-person related users that allows the assignment of additional identical authorizations, such as for Internet users created with transactions SU01. You cannot log on to the system with a reference user.
- To assign a reference user to a dialog user, specify it when maintaining the dialog user on the Roles tab page. In general, the application controls the assignment of reference users. This assignment is valid for all systems in a Central User Administration (CUA) landscape. If the assigned reference user does not exist in a CUA child system, the assignment is ignored.
- You should be very cautious when creating reference users.

Role vs Profile

- Important!!!,
- SAP Security Interview questions

Role refers to the collection of associated activities as transactions, reports and so on.
While profile is a set of authorizations that are valid for the transactions defined in that role.

Role has various components as MENU of transaction, reports, urls; AUTHORIZATION PROFILE(S) and USERS who are assigned to that role.

Roles are otherwise called Activity Groups or User Role Templates.

Maintenance Status of an Authorization

- Important!!!,
- SAP Security Interview questions,
- Tac n Ticks

Standard:
• All field values in the subordinate levels of the hierarchy are unchanged from the SAP defaults
• This includes both filled and unfilled organizational level fields.
Maintained:
• At least one field in the subordinate levels of the hierarchy was empty by default and has since been filled with a value.
Changed:
• The proposed value for at least one field in the subordinate levels of

the hierarchy has been changed from the SAP default value.
Manual:
There maintained at least one authorization in the subordinate hierarchy
levels manually (it was not proposed by the Profile Generator).
Before you make a change to authorizations that generates the status.
Changed, you must first perform the following steps:
1. Copy the relevant specification.

2. Set the template to inactive.

3. Make the changes to the copy

Only by performing these steps can you avoid the default being read again
and again, and ensure that you have no inexplicable values to maintain.
Status texts after a comparison.
Old: The comparison found that all field values in the subordinate levels of the hierarchy are still current and that no new authorizations have been added.
New: The comparison found that at least one new authorization has been
added to the subordinate levels of the hierarchy. If you now click New, all new authorizations in the subordinate levels are expanded.

Expert mode options:

- Important!!!,
- Tac n Ticks

- ***Delete and recreate profile and authorizations***

– All authorizations are recreated. Values which had previously been maintained, changed or entered manually are lost. Only the maintained values for organizational levels remain.

- ***Edit old status***

– The last saved authorization data for the role is displayed. This is not useful, if transactions in the role menu have been changed.

- ***Read old status and compare with new data***

– If you change transactions in the role menu, this option is the preconfigured. The profile generator compares the existing authorization data with the authorization default values for the menu transactions. If new authorizations are added during this process, they receive the status *New*. Authorizations that already existed receive the status *Old*.

SAP_ALL and SAP_NEW

- Important!!!,
- SAP Security Interview questions

SAP_ALL is a SAP standard profile, which is used on need basis, to resolve particular issues which may arise during the usage of SAP. It is used by Administrators/Developers only and is

applied on a need to use basis, then withdrawn. It contains all SAP system objects and Transactions. SAP_ALL is very critical and only SAP* contains SAP_ALL attached to it in the production system. No other dialog users have SAP_ALL attached to them.

SAP_NEW is a SAP standard Profile which is usually assigned to system users temporarily during an upgrade to ensure that the activities and operations of SAP users is not hindered, during the Upgrade. It contains all the necessary objects and transactions for the users to continue their work during the upgrade. It should be withdrawn once all upgrade activities is completed, and replaced with the now modified Roles as it has extensive authorizations than required.

SAP_NEW is used in the Production environment during a version upgrade whereas SAP_ALL shouldn't be or not allowed be used in Production (for audit purposes obviously), except where necessary, in a controlled manner with all proper approvals from the customer.

Profiles in SAP

- Important!!!,
- SAP Security Interview questions

SAP profiles are operating system files that contain instance setup information. SAP Systems can consist of one or more instances. Individual setup parameters can be customized to the requirements of each instance.

Start Profiles

When you start an SAP instance on a host, the start profile defines which SAP services are started (message server, dialog, gateway or enqueue process. for example). The **startsap** program is responsible for starting these service processes, and it uses a start profile to begin the startup process.

The processes that can be started include:

- Application server
- Message server
- SNA Gateway
- System log send demon
- System log receive demon

Default Profiles

If you want to assign the same parameter value for all application servers (such as the name of the database host, or the host on which the message server is running), enter it in the default profile.

You **cannot** choose a name for the default profile. It is always called **DEFAULT.PFL** . Default profiles are also called **system profiles**.

Instance Profiles

nstance profiles provide an application server with additional configuration parameters to complement the settings values from the **default profile**. Typically, these parameter settings adapt the instance according to the desired resources. They also define the available instance resources (main memory, shared memory, roll memory and so on), and how to allocate memory to the SAP application buffers.

You can choose any name for an instance profile. The SAP naming convention is as follows: **<SID>_<instancename>** or **<SID>_<instancename>_<hostname>** .

To start application servers on several computers using identical parameter settings, you can use a single instance profile. It is generally not necessary for each application server to have its own instance profile. Instance profiles are also called **system profiles**.

Diff. between Customized and Workbench request?

- Important!!!,
- SAP Security Interview questions,
- Tac n Ticks

The Transport Organiser maintains Change Requests.These requests record the changes made to the repository and customizing objects.Based on teh objects changed they are

- **WorkBench Request &**
- **Customizing Request.**

Workbench Requests are those that involve changes to cross-client Customising and Repository Objects. The objects are independent of the client.Hence the requests are used for transferring and transporting changed Repository objects and changed system settings from cross-client tables.

Customizing Requests involve changes recorded to client-specific Customizing objects .These client specific requests are used for copying and transporting changed system settings from client-specific tables.

User Creation Date… !!!

- Important!!!,
- SAP Security Interview questions,
- Tac n Ticks

Table USR02 is the answer.

USR02-GLTGV (field) is the date from when user is permitted to use the system.

So let suppose if you created the UserID on 01/01/2011 and wants to allow him/her from 03/01/2011 then user creation date would be 01/01/2011 but USR02-GLTGV holds the value 03/01/2011 .

Actually user creation date is **USR02-ERDAT**.

Lock Value In USR02

- General,
- Important!!!,
- SAP Security Interview questions,
- Tac n Ticks

Actually, this information is new for me. I got this question in an Interview.

I knew that except '0′ (Zero) rest are locked. But there are some value which is maintained in USR02 when user is locked by different user/purpose.

We use **USR02** table for checking the status of an user whether user is locked or not.

There are 6 type of values are there.

0	Not locked
16	Mystery values
32	Locked by CUA admin (User Admin)
64	Locked by system Administrator
128	Locked due to incorrect logon attempts or too many failed attempts
192	A combination of both. The user is locked by admin and user tries to logon with incorrect passwords and gets locked (192 = 64+128)

SU22 Vs SU24

- SAP Security Interview questions,
- SAP Security- Authorizition,
- Tac n Ticks

SU22 displays and updates the values in tables USOBT and USOBX, while SU24 does the same in tables USOBT_C and USOBX_C. The _C stands for Customer.

The profile generator gets its data from the _C tables. In the USOBT and USOBX tables the values are the SAP standard values as shown in SU24. With SU25 one can (initially) transfer the USOBT values to the USOBT_C table.

Add T-CODE IN Role MENU Vs Add T-CODE in S_TCODE OBJECT

- Important!!!,
- SAP Security Interview questions,
- SAP Security- Authorizition

What is diffrence between add T-CODE IN ROLE MENU (PFCG) and add T-CODE in S_TCODE OBJECT IN TCD field?

Roles are basically **graphical interface** of an end-users. If you add some role in PFCG Menu then end-user will show a link in end users Screen.

Even end-users don't know which T-CODE is calling for clicking a link in his/ her screens. and link will appear only when ROLE will assigned to user.

But when you add a T-CODE in **S_TCODE** in **TCD** fields then user is able to run the query in backend (sap logon pad), not from the end-user screen cause no **LINK** will come for that.

So, when you enter a T-CODE in PFCG screen it will automatically added to object S_TCODE, but opposite is not true.

Suppose you have a profile SAP_ALL, you can do anything in backend (using SAP LOGON PAD). but when you assigned this to a end-user, he/she should not get any link to their screens (it's a profile not Role).

Like, we are in Security Module, we have access for User and Role administration. but a person Like Sales Supervisor, he/she don't know even what are the background behind that, he/she knows only if he clicks some link he can perform some job.

Add T-CODE IN Role MENU Vs Add T-CODE in S_TCODE OBJECT

- Important!!!,
- SAP Security Interview questions,
- SAP Security- Authorizition

What is diffrence between add T-CODE IN ROLE MENU (PFCG) and add T-CODE in S_TCODE OBJECT IN TCD field?

Roles are basically **graphical interface** of an end-users. If you add some role in PFCG Menu then end-user will show a link in end users Screen.

Even end-users don't know which T-CODE is calling for clicking a link in his/ her screens. and link will appear only when ROLE will assigned to user.

But when you add a T-CODE in **S_TCODE** in **TCD** fields then user is able to run the query in backend (sap logon pad), not from the end-user screen cause no **LINK** will come for that.

So, when you enter a T-CODE in PFCG screen it will automatically added to object S_TCODE, but opposite is not true.

Suppose you have a profile SAP_ALL, you can do anything in backend (using SAP LOGON PAD). but when you assigned this to a end-user, he/she should not get any link to their screens (it's a profile not Role).

Like, we are in Security Module, we have access for User and Role administration. but a person Like Sales Supervisor, he/she don't know even what are the background behind that, he/she knows only if he clicks some link he can perform some job.

When to use SU24?

- Important!!!,
- SAP Security Interview questions,
- SAP Security- Authorizition

- To correct authorization objects that are not linked to transaction codes correctly

- To correct authorization objects that have unacceptable default values.

- To change default values to ones that will always be appropriate for all roles that will ever use the transaction. This means having blank fields where you need to allow different roles to have different values.

How SAP R/3 security is different from SAP BW and EP

- BW Security,
- SAP Security Interview questions,
- SAP Security- Authorizition,
- Tac n Ticks

Security in SAP BW, Enterprise Portal and SAP HR is quite different from the SAP R/3 Security.

BW : In SAP BW there are primarily two different types of authorization objects. The standard authorization objects that are provided by SAP and cover all checks for e.g. system administration tasks, data modeling tasks and granting access to InfoProviders for reporting.

This type of authorization has the same concept and technique as that of an R/3 system. The second type of authorization objects is used for granular authorization checks on an Info

Provider's data and is defined by the customer. These reporting authorization objects can be used to specify which part of data within an InfoProvider is visible to a user. Both types of authorization objects use the same authorization framework.

Technically they are treated in the same way. However, the design of reporting authorizations is more complex because of the need to design the reporting authorization objects first. This is an additional step that needs to be treated with care because the structure of the authorization objects determines the possible use in regards to selections, combinations and granularity.

Enterprise Portal : SAP Enterprise Portal provides a bunch of capabilities to the end users—with uniform, role-based, and secure access to their day-to-day work and information resources through a Web-based portal interface. These resources include SAP applications, third-party applications, databases, data warehouses, desktop documents, Web content, and services. The portal makes it possible to search internal and external sources, and to access both structured and unstructured information from any geographical location throughout the organization.

The portal has an authorization concept that is implemented using permissions, security zones, UME actions, and the AuthRequirement property.

Permissions: permissions for all Portal Content Directory (PCD) objects. Portal permissions define portal user access rights to portal objects in the PCD and are based on access control list (ACL) methodology.

Security Zones: Control which portal components and portal services users can launch and are defined in the development phase. If a portal component or service is not assigned a complete security zone in its descriptor file, the portal runtime assigns it to a predefined security zone folder for unspecified components or services.

UME Actions: the User Management Engine (UME) equivalent of portal permissions. The UME verifies that users have the appropriate UME actions assigned to them before granting them access to UME iViews and functions.

Auth Requirement property: This is a master iView property used in EP that defines which users are authorized to access a master iView or Java iViews derived from a master iView. For backward compatibility with iViews developed for EP 5.0, EP 6.0 supports this property.

Usually the sap standard tables USOBX and USOBT are not allowed modifications so that we copy the customized tables from these tables so in order to copy the tables we need to go the transaction su25.

su22 displays and update the values in standard tables USOBT, USOBX.

su24 displays and update the values in customizing tables USOBT_C, USOBX_C.

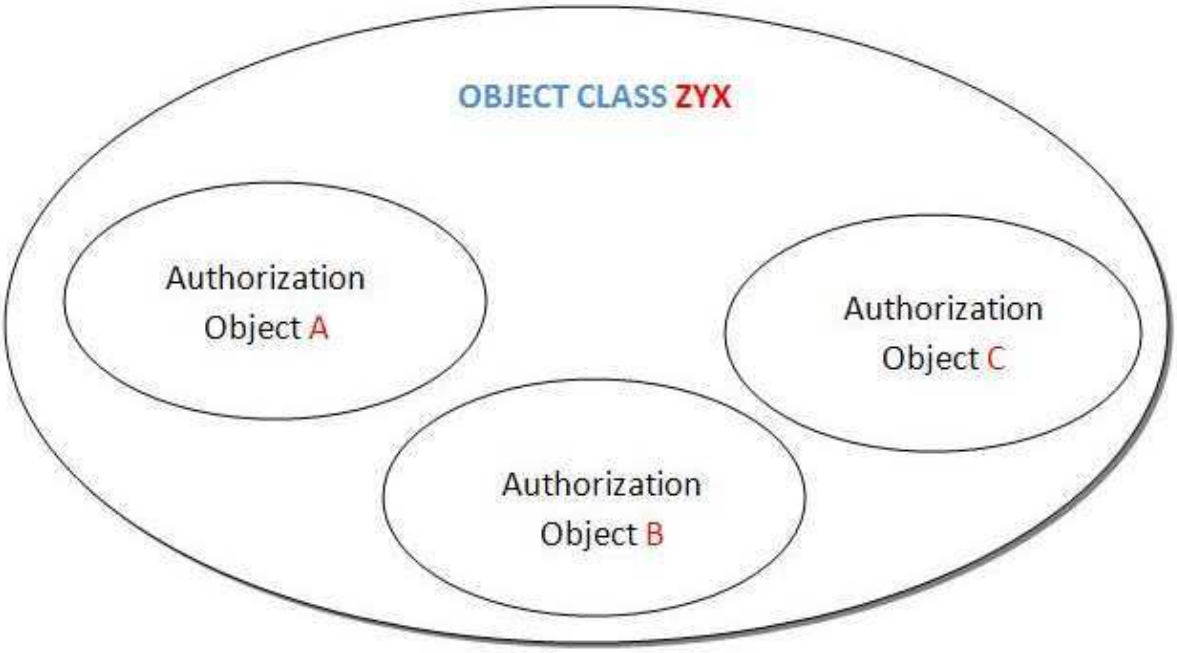
How Authorization Object Works !!!!

- SAP Security Interview questions,

- SAP Security- Authorizition,
- Tac n Ticks

The Authorization Object mechanism is used to inspect the current user's privileges for specific data selection and activities from within a program.

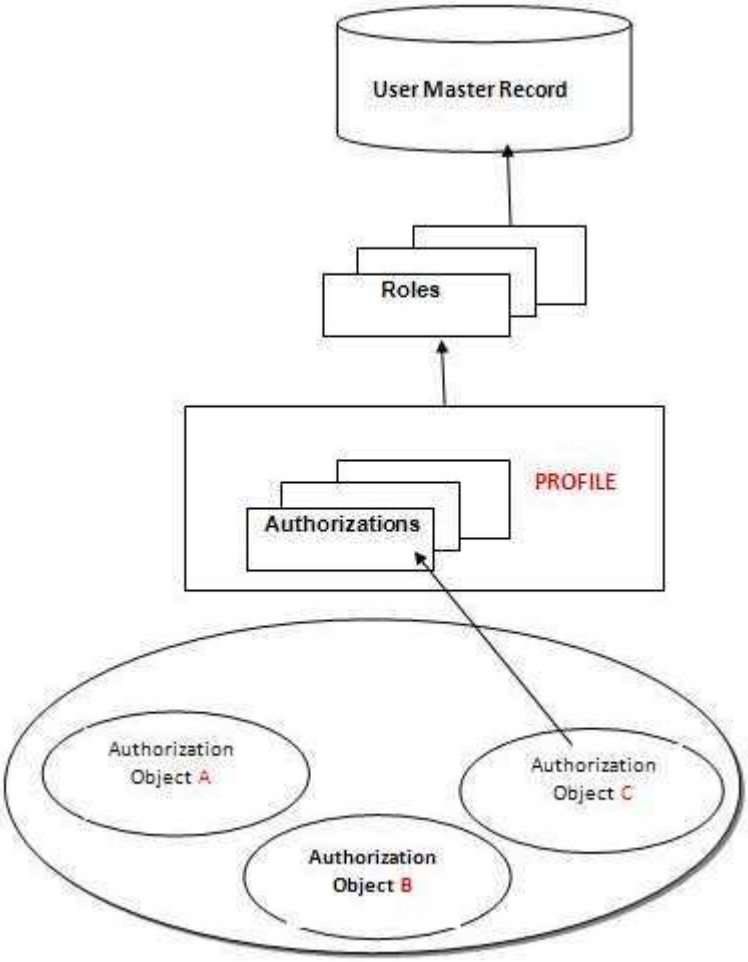
An **Object Class** contains one or more **Authorization Objects.**



The Authorization Object is where **Permitted Activity configurations are performed against specific fields**.

Before a User can be granted permission by the **Authorization Object**, the **User's Master Record** is assigned a **Role**, which includes a **Profile**.

The Profile contains what is simply called the **Authorization** and is where the specific data for the **Authorization Object's field** is assigned to the configured Permitted Activity.



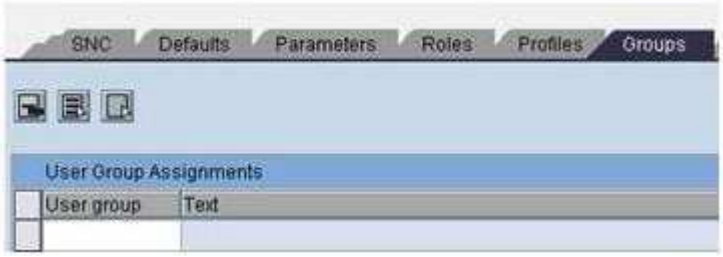
Finally the calling of the **Authorization Object** can me performed in code.

User Groups

- Important!!!,
- SAP Security Interview questions,
- SAP Security- Authorizition,
- Tac n Ticks

User groups are basically an instrument for the user administration, but you can also utilize them for internal organization of users. Users can be assigned to multiple user groups.
The user groups are generally maintained via transaction **SUGR**.
We have two different fields for user groups in the user master [transaction **SU01**]:

1. *Groups – on the groups tab*



This field is for the internal organization of users and helpful e.g. For mass maintenance – if you want to maintain users of a certain group. This group is also called the ***General user group*.**

2. *User groups for authorization check – Logon tab*

This field allows to restrict user maintenance to specific groups based on the authorization object **S_USER_GRP**. If a user has an assignment maintained in this field, the user administrator will need the corresponding group assigned to his authorization based on **S_USER_GRP** to be able to actually maintain this user.

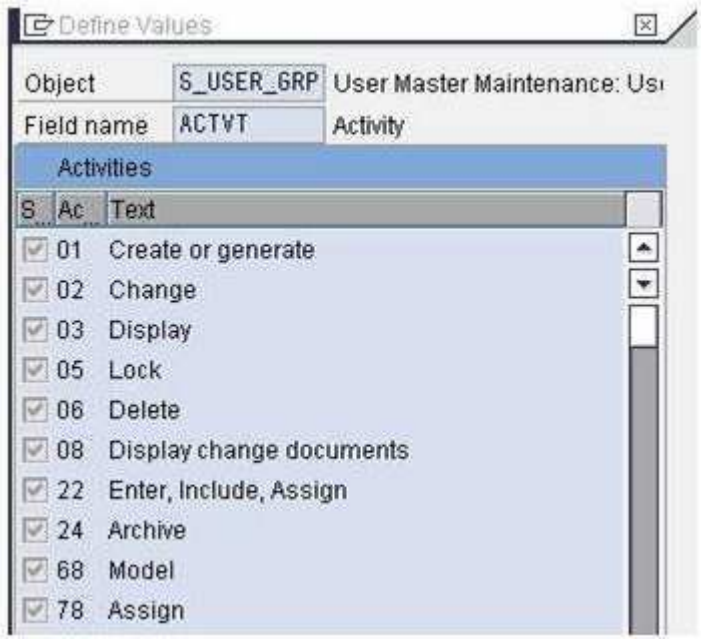
***Example*:**

The user ***Z_ZYX*** is assigned to the group ***TCS***.

The user administrator who wants to maintain this user ***Z_ZYX*** will need the authorization:

S_USER_GRP
with ACTVT = *02* [change]
with CLASS = *TCS*

The activities that are available for defining the access level on **S_USER_GRP** are the following:

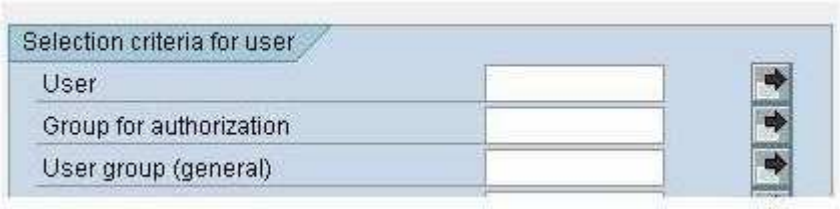


What do they have in common – what is different?

The user groups are generally maintained via transaction **SUGR**.
Though both described fields pull the information from the same table **USGRP**, only the entries in *User group for Authorization Checks* are actually relevant for checks on **S_USER_GRP**.

The information for *User group for Authorization Checks* is also stored in the table **USR02** in the field **CLASS** [User group] whereas the assignment for the field *General user groups* is stored in the table **USGRP_USER**, and can be displayed via **SE16.**

The report **RSUSR002** allows to distinguish and select users based on the respective group information.



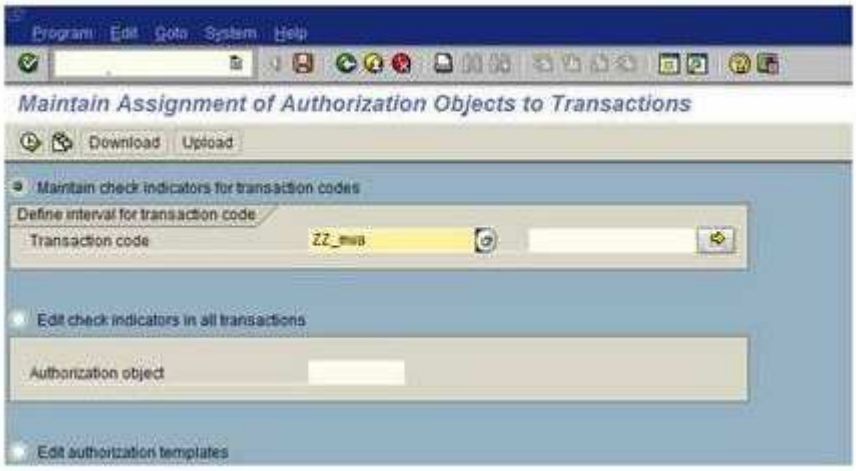
Everybody knows about USER GROUP. But I think It should give some extended information of USER GROUP. Thanks.

How to add an authorization object to New created TCODE

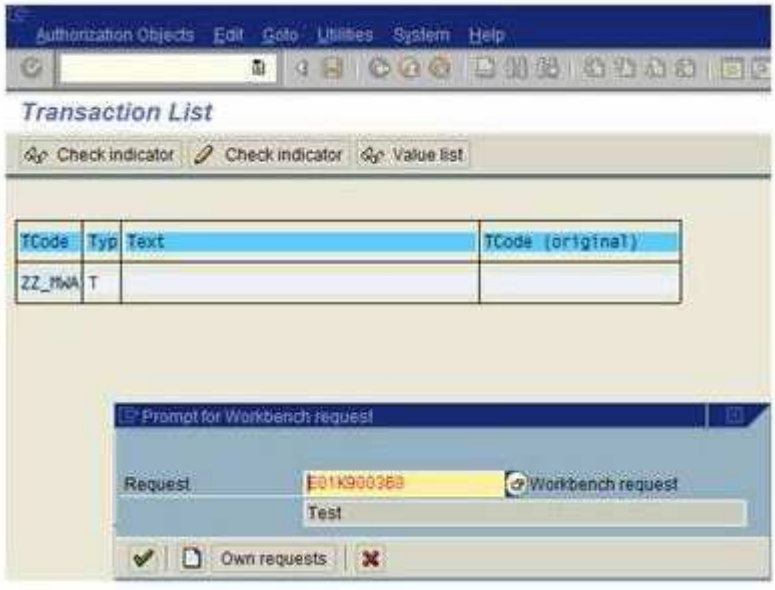
When you are creating a TCODE, it doesn't have any AUTH OBJ (except S_TCODE, This check always takes place and cannot be deactivated by the developer). So we have to manage the tcode using Adding AUTH OBJ. Call the transaction **SU24** to start the maintenance.

The transaction in this example currently consists of only one authorization object (S_TCODE) and is not listed in the table **USOBT_C** yet.

Select the transaction you want to maintain.



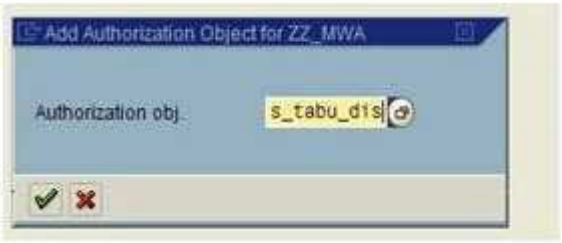
Confirm your choice via Execute(*F8)* and double click the selected entry.
The following message will be displayed.



Confirm the message with *Enter*. Select the target client. Enter your request ID and confirm via *Enter*.

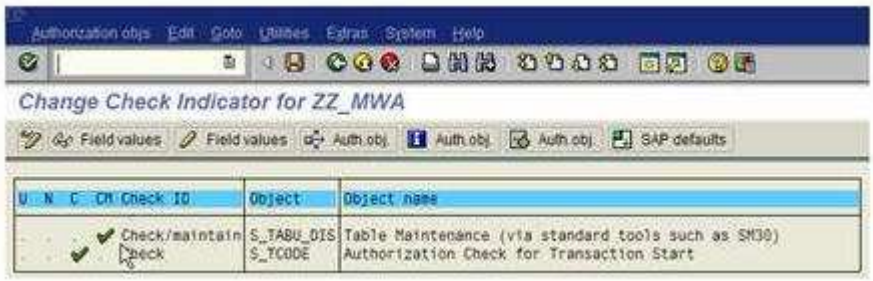
Select the item Authorization objects from the menu bar, and there the entry *Insert*.

Choose the corresponding authorization object from the list , or enter it directly.



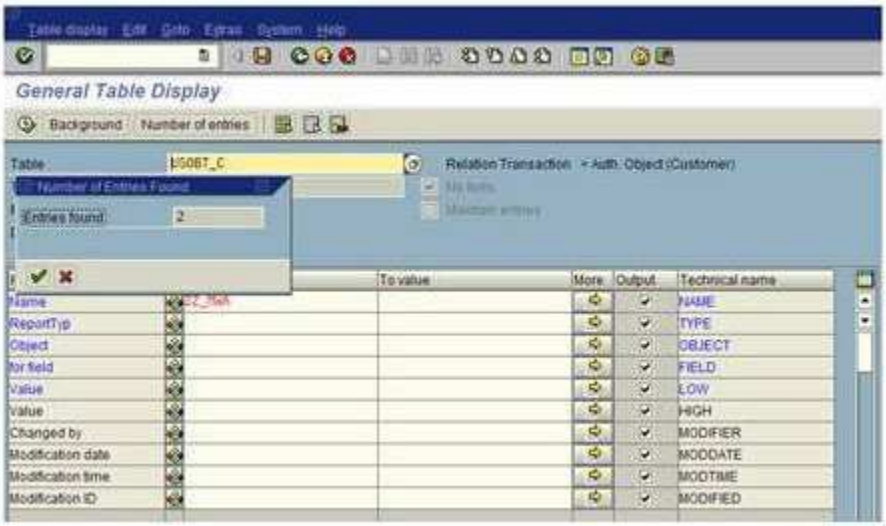
Confirm your choice.

The selected authorization object will be transferred to the list. If you want this object to be called by the profile generator for maintenance you have to adapt the Check ID.

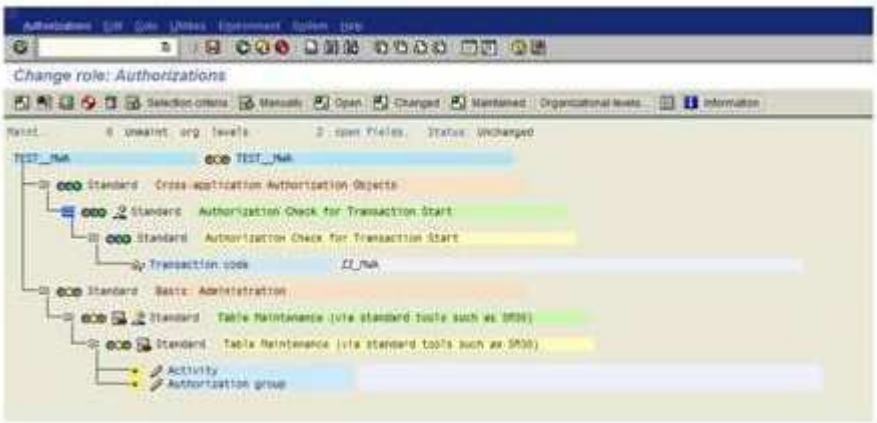


When you are finished with the maintenance – save the adjustments.

At the call of the transaction **SE16N /SM31** with selection of the table **USOBT_C,** the maintained values for the corresponding transaction
are added to the table.



At the call of the profile generator **[PFCG]** with selection of the previously maintained self-created transaction, the adapted check values are displayed for further maintenance.



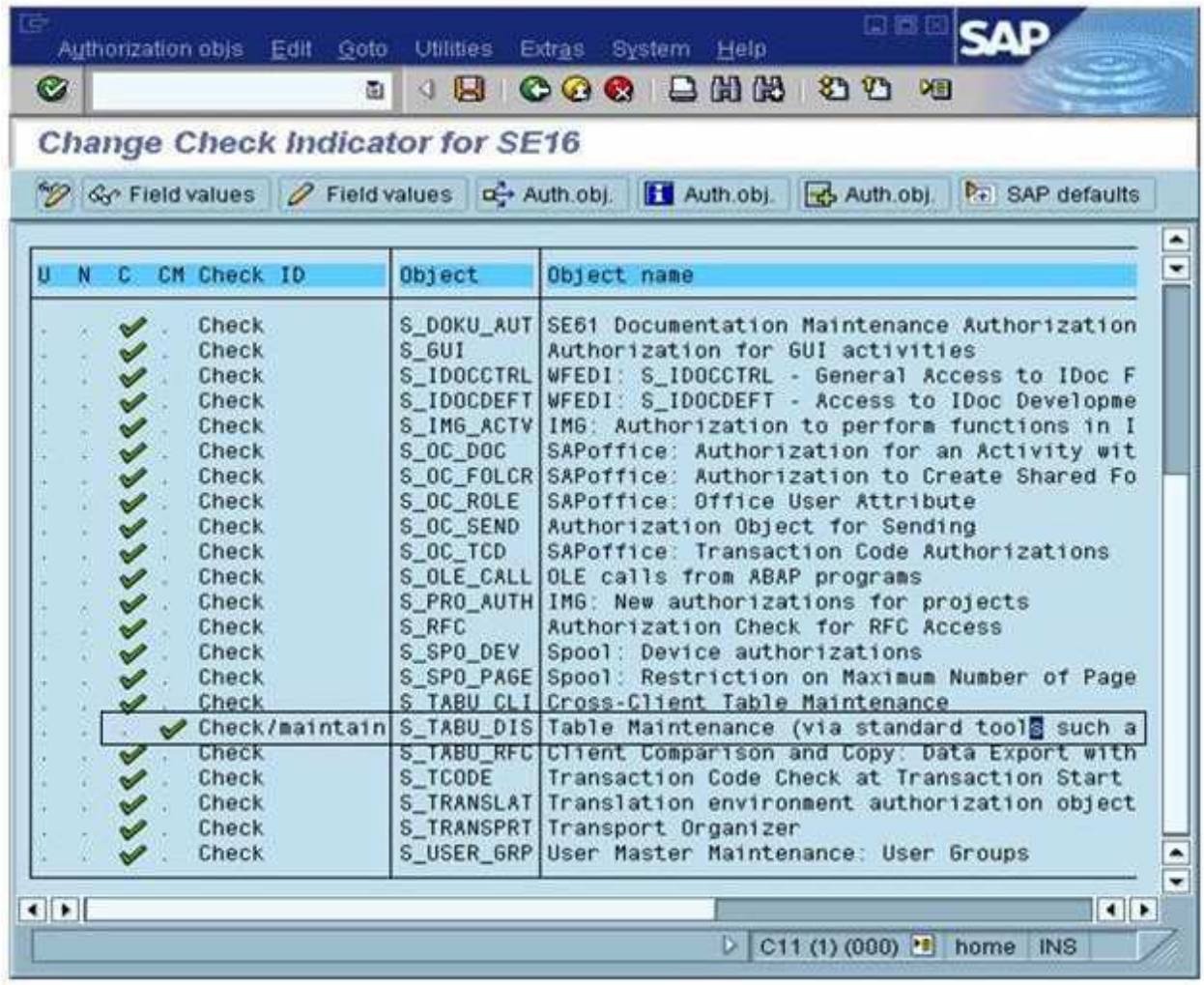
Restricted Security to SE16 – Data Browser.!!!

- Important!!!,
- SAP Security- Authorizition,
- Tac n Ticks

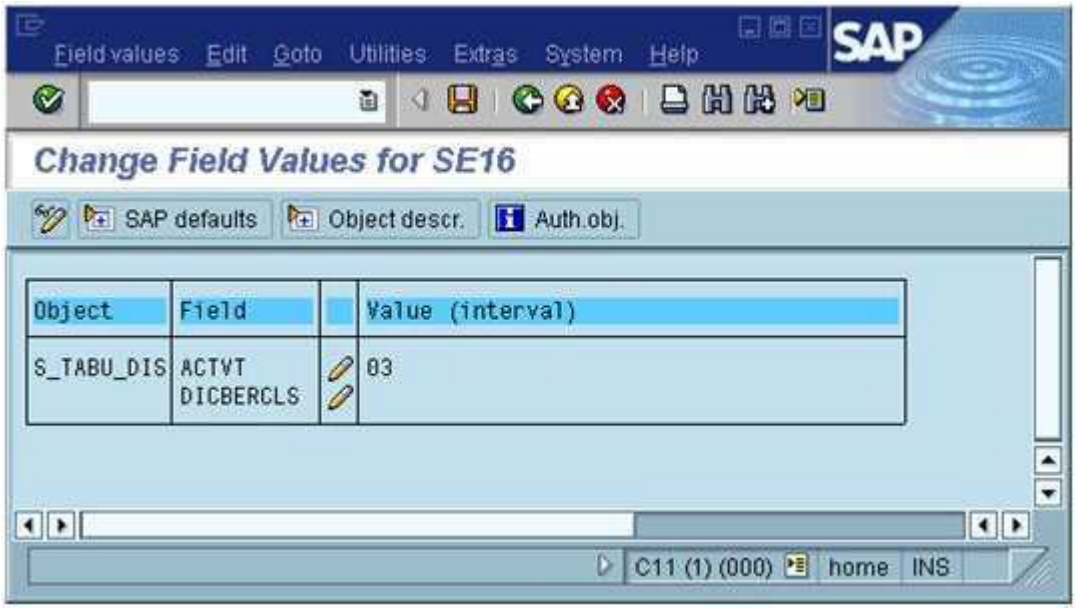
Suppose we have to create a Role that can only have **Data Browser t code (SE16) with table USR02** and **AGR_USERS *DISPLAY* ACCESS**.

In SE16, only one authorization object (**S_TABU_DIS**) is check maintained in **SU24**.

SU24 screen for SE16.



Display Field values for S_TABU_DIS Screen:



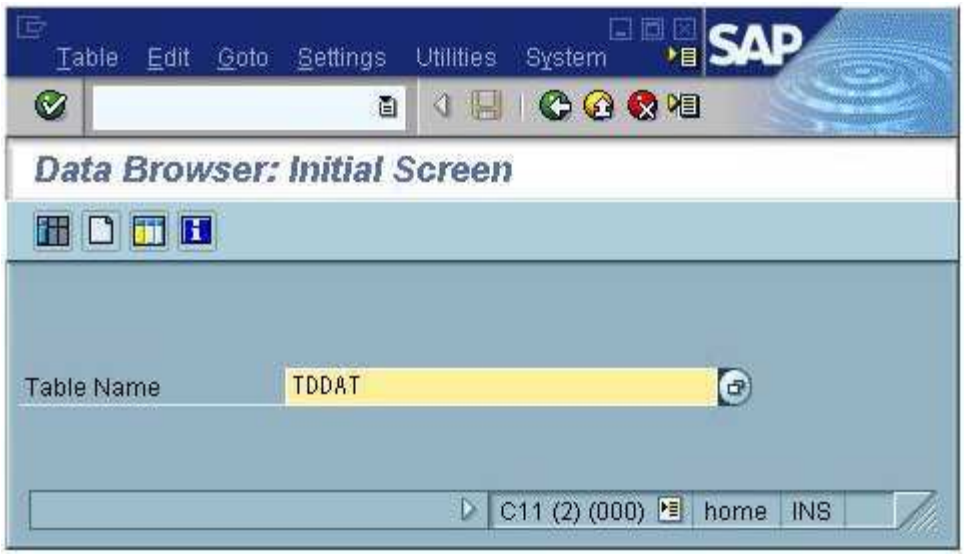
Here ACTVT =03 AND DICBERCLS (AUTH GROUP) is blank. so when PFCG (ROLE Maintenance) pull the data from SU24 for SE16 the object **S_TABU_DIS** will be yellow.

(For more details go to "What does the different color light mean in profile generator ")

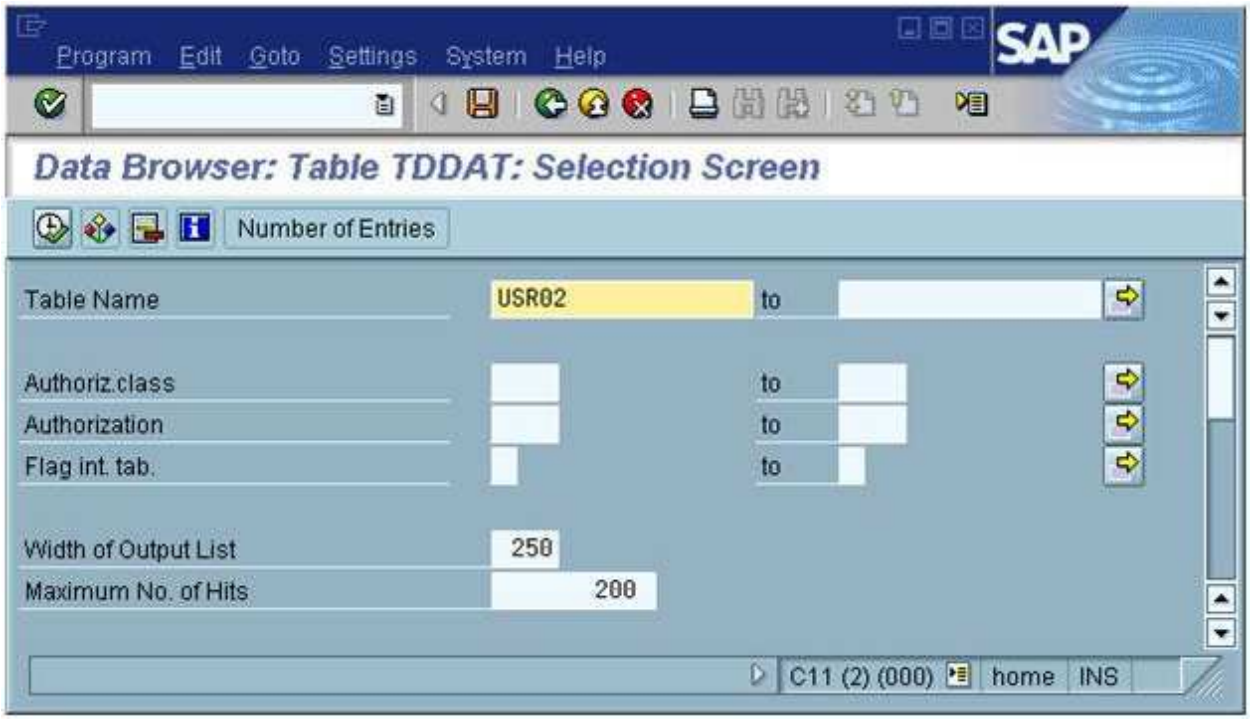
Lets create the Role **Z_TCS**.

Before that we have to check, what are the **AUTHORIZATION GROUP** for those tables (**USR02 and AGR_USERS**).

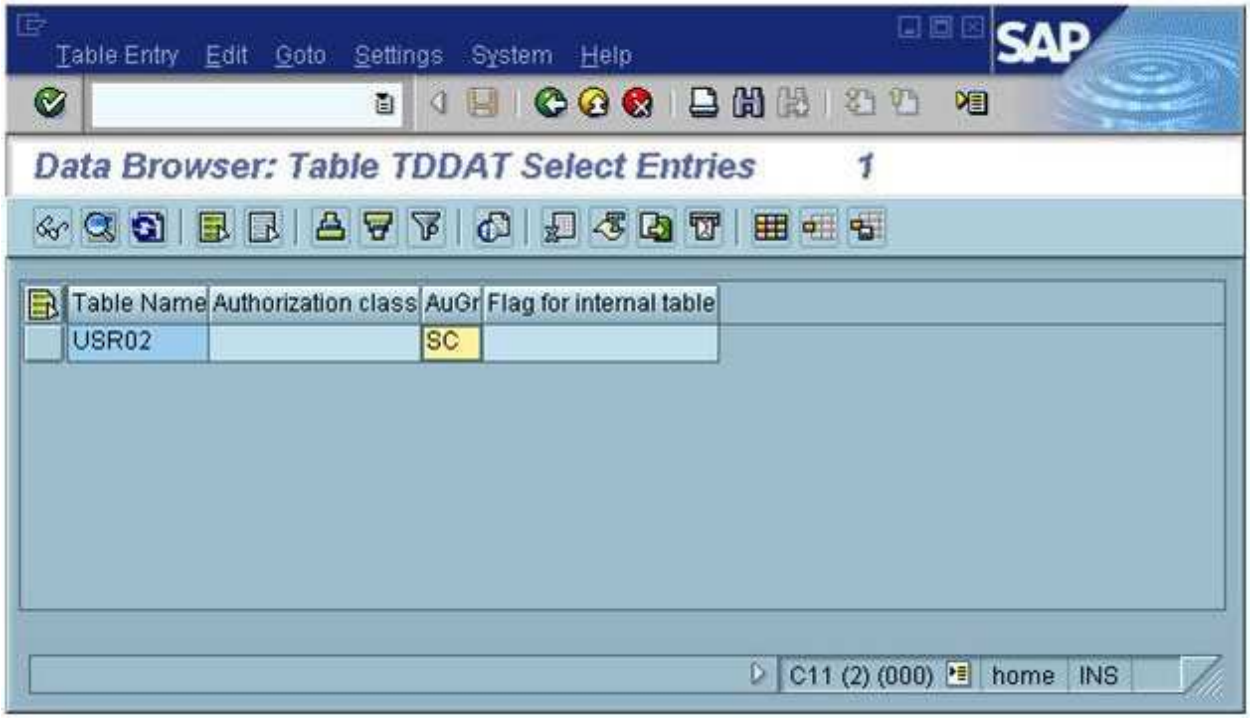
So goto Data Browser (SE16) and Type Table TDDAT. It stores Table auth group.



Put table name USR02.

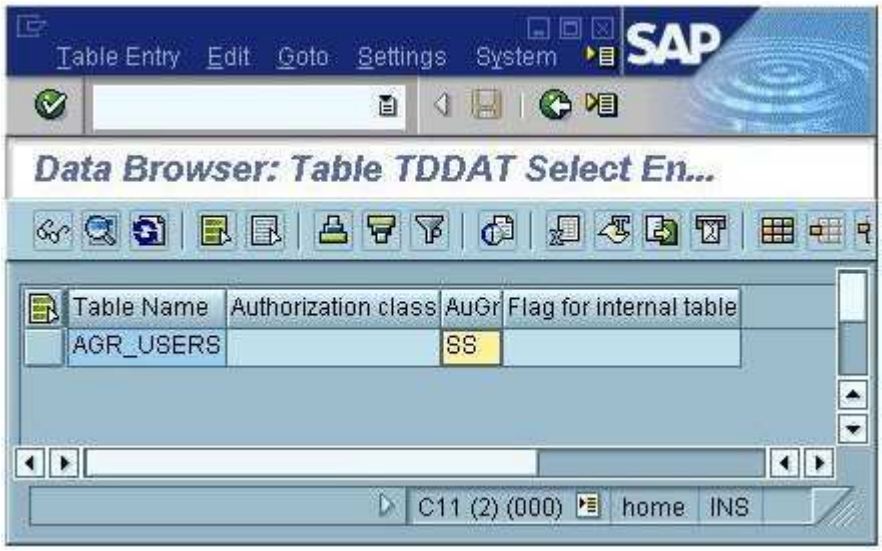


And then execute.

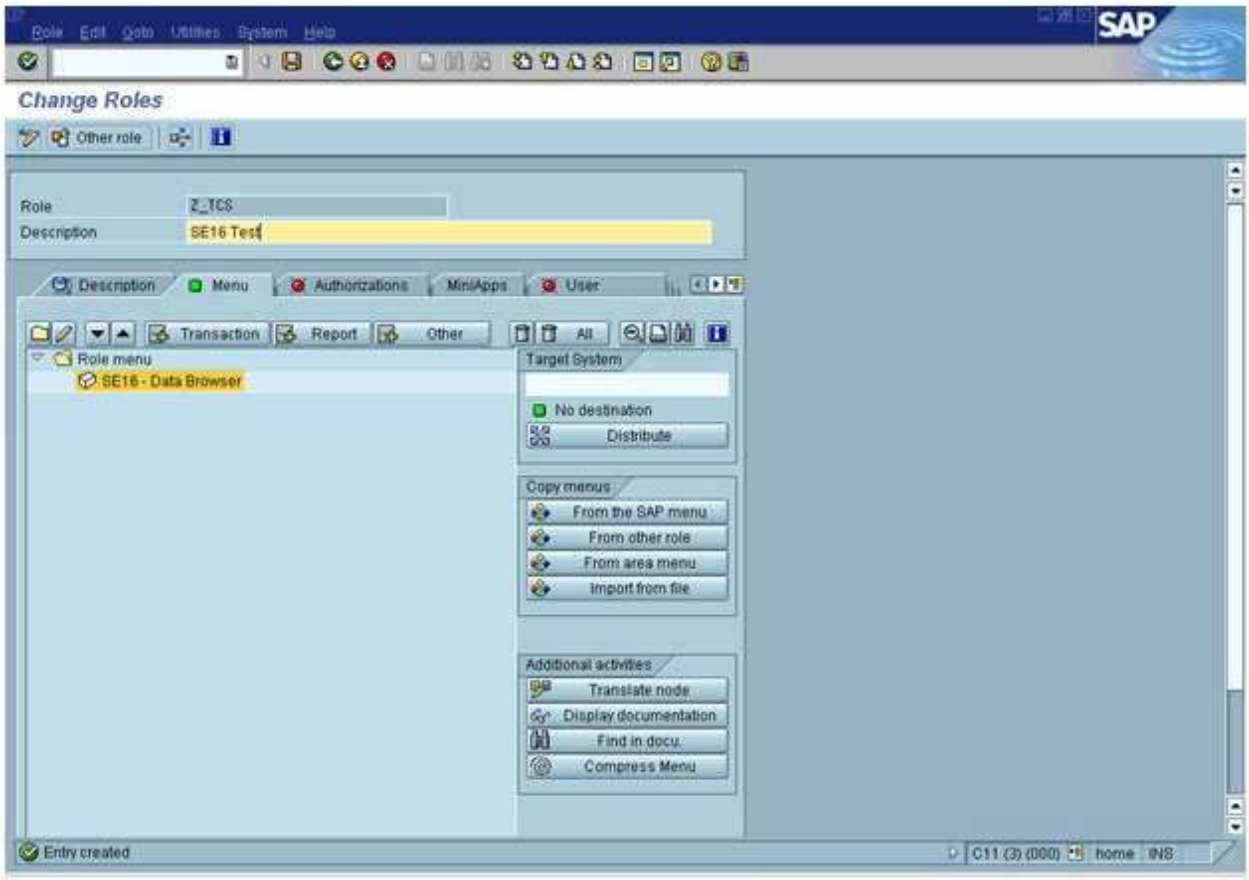


So, we get SC is the auth group for the table USR02.

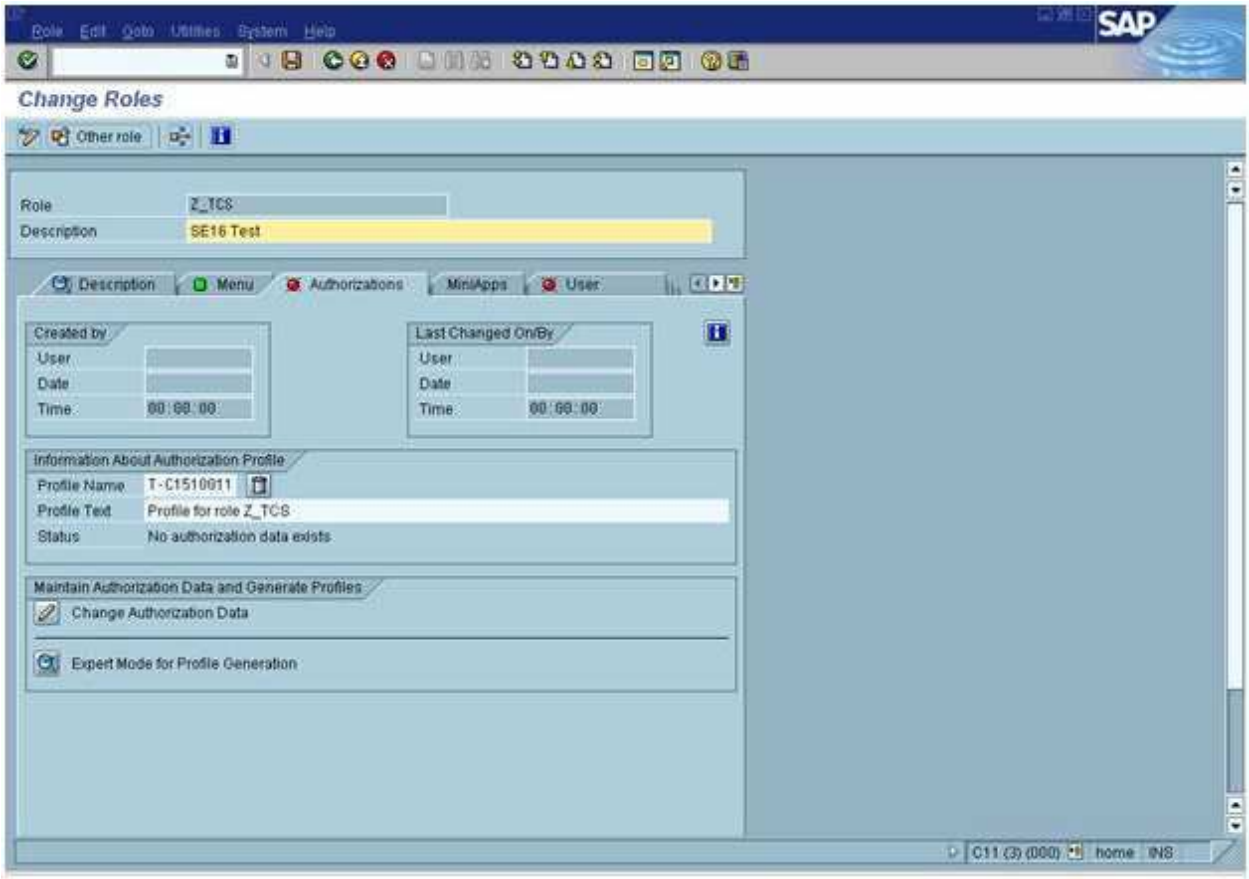
And SS is the auth group for table AGR_USERS.



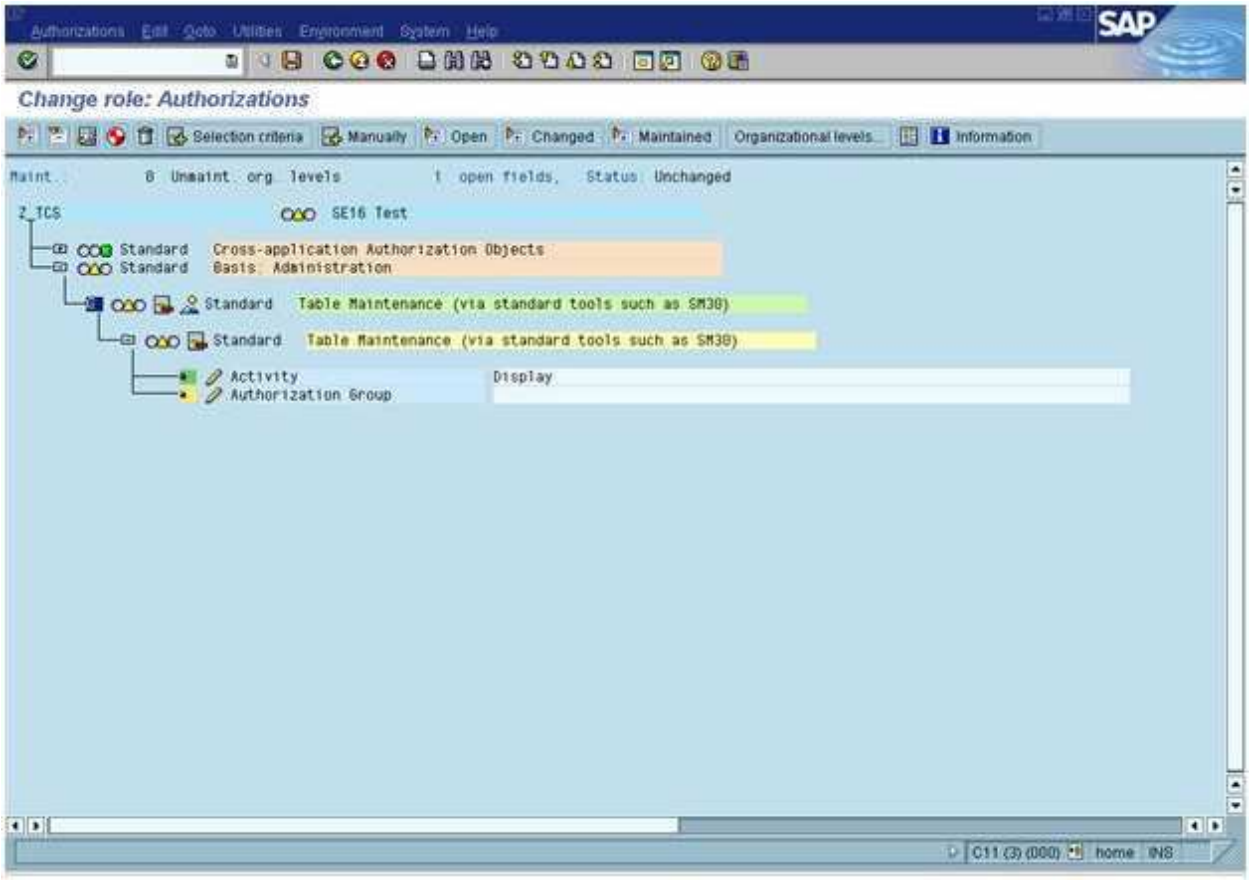
Now add transaction code SE16 to the Role Z_TCS.



Now goto authorization tab and fill the profile name and click **CHANGE AUTHORIZATION DATA**.



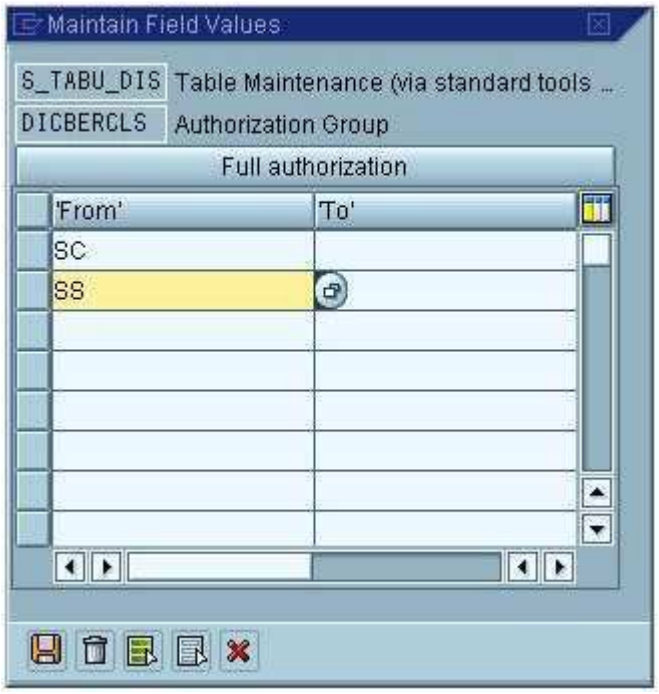
Search S_TABU_DIS, and Authorization Data will display like this.



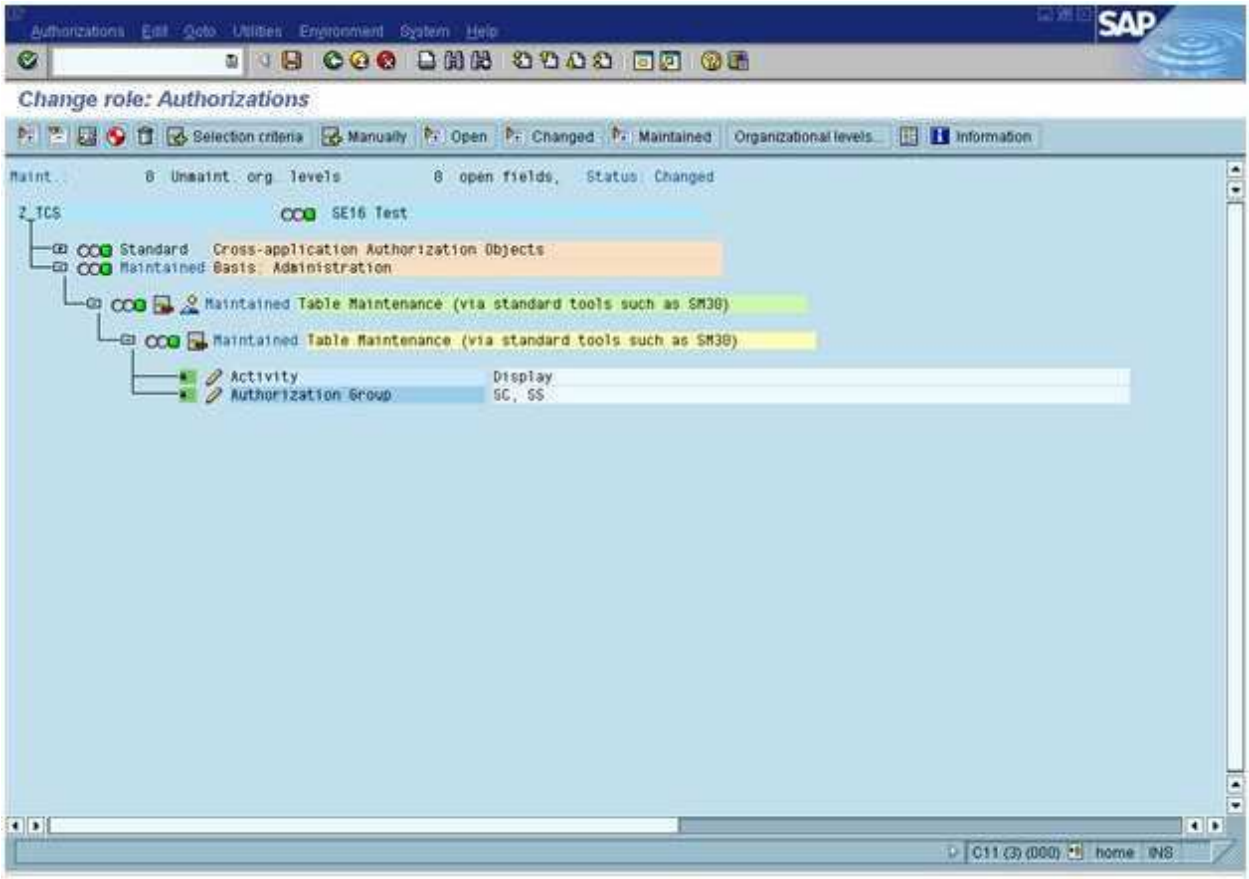
That’s the Yellow Object !!!!!

So you have to maintain those field values, change **DICBERCLS (AUTH GROUP)**.

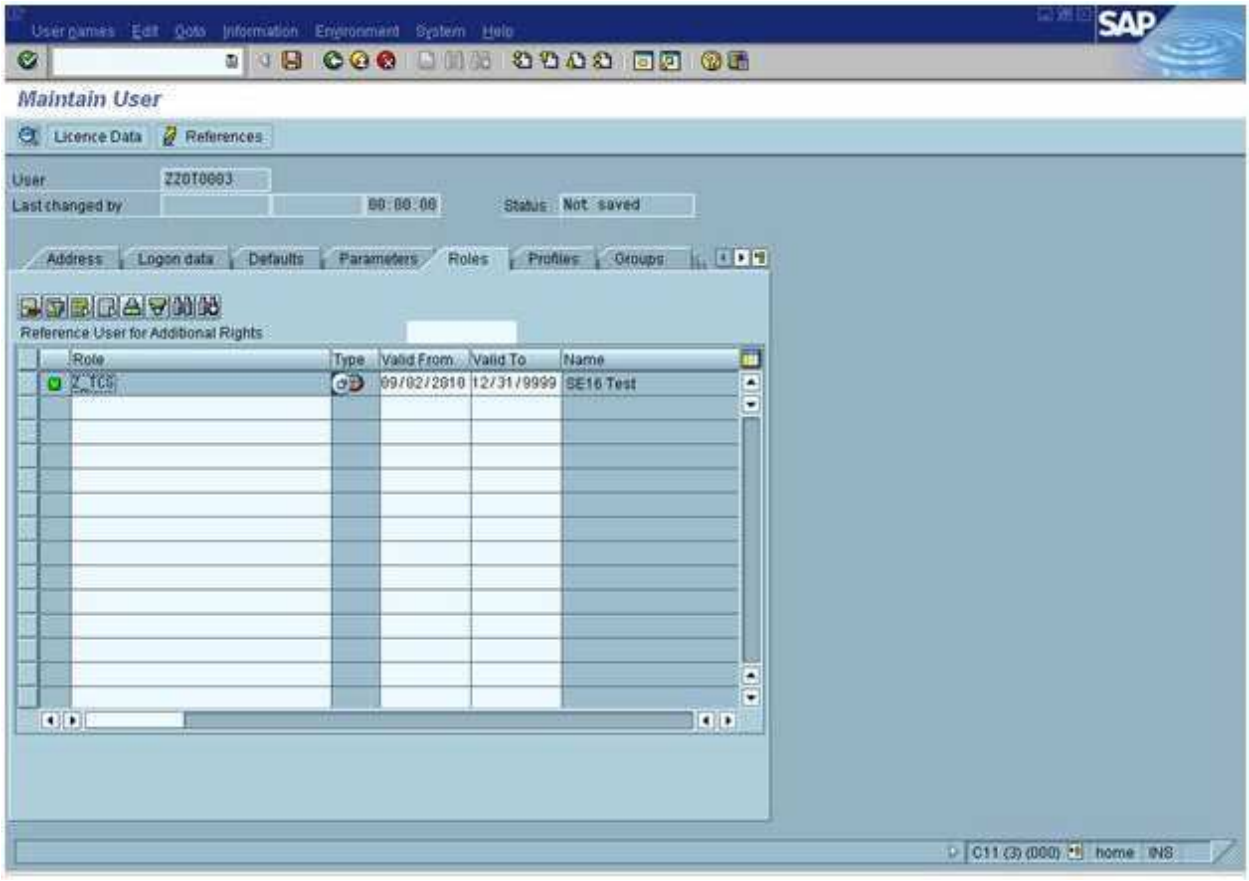
Goto change (pencil Icon) to **DICBERCLS** field. And add those two **AUTH GROUP** (SC and SS).



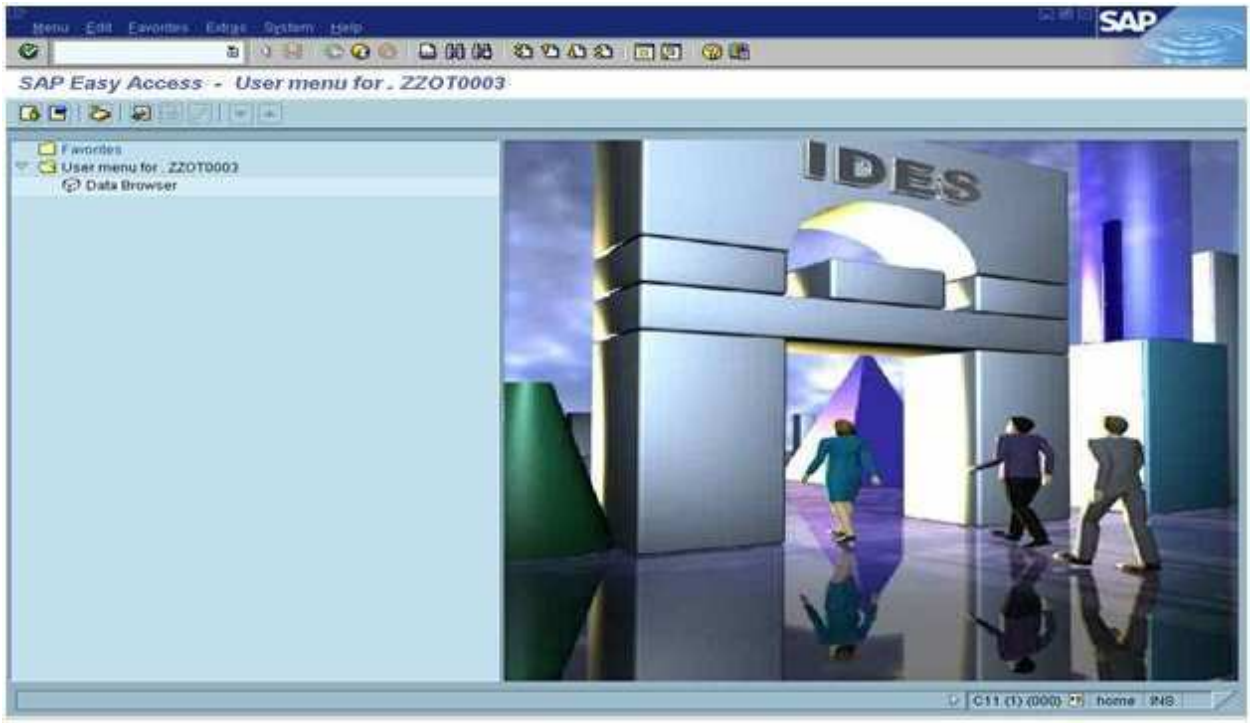
And save it and Generate the Role. And it will look like …….



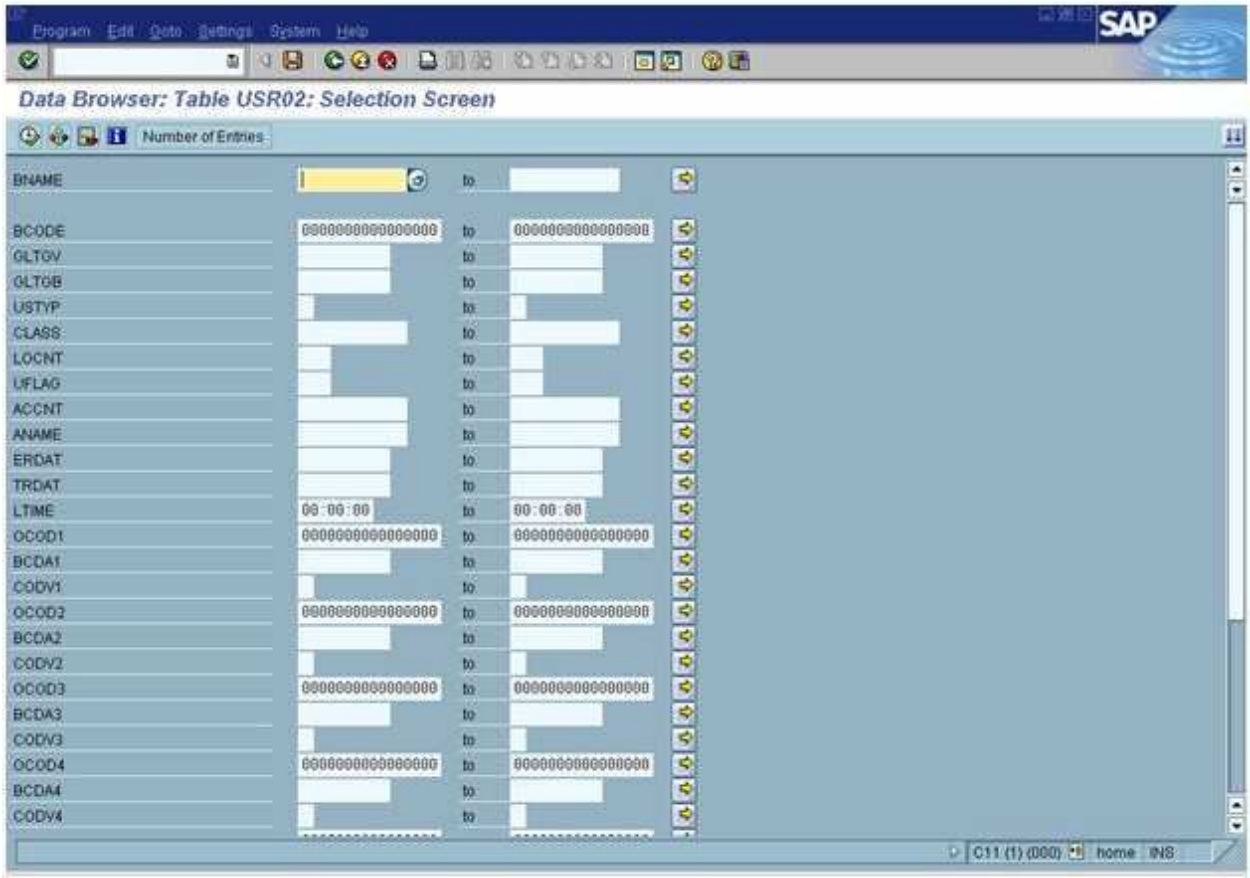
Now create a USER ZZOT0003, and assign role **Z_TCS** to the user.



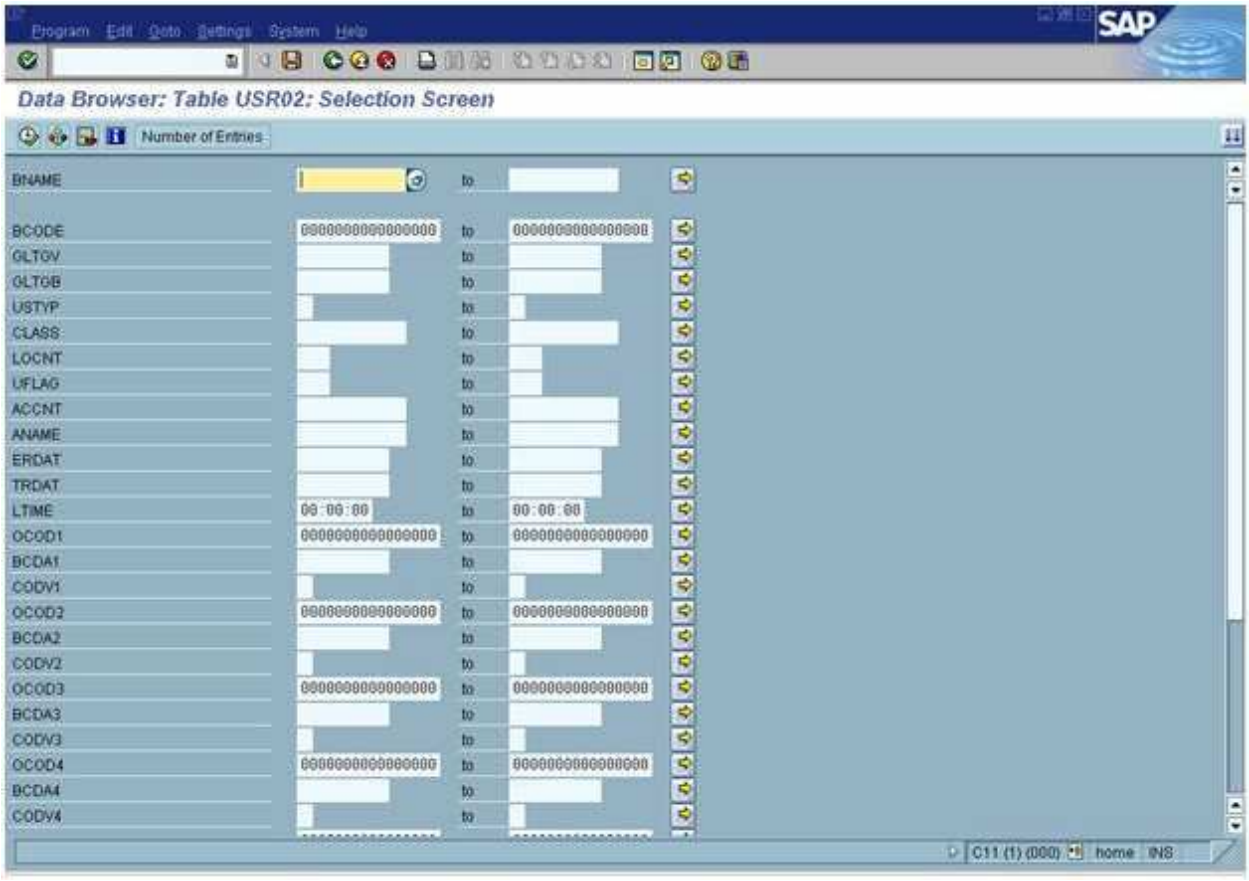
Now Login through the user ZZOT0003.



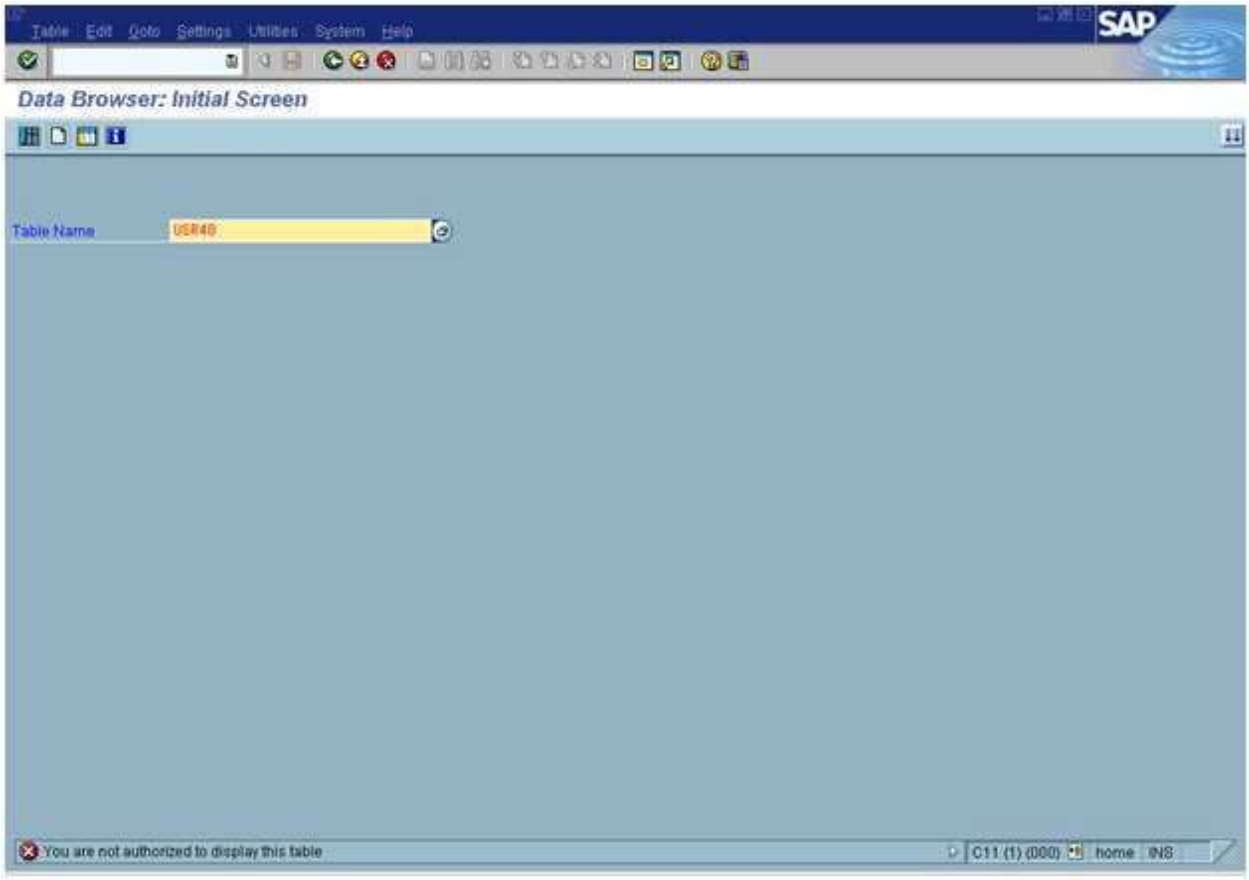
Now Run SE16 and Put the table USR02. It will execute without authorization error.



And table AGR_USERS will also display without authorization error.



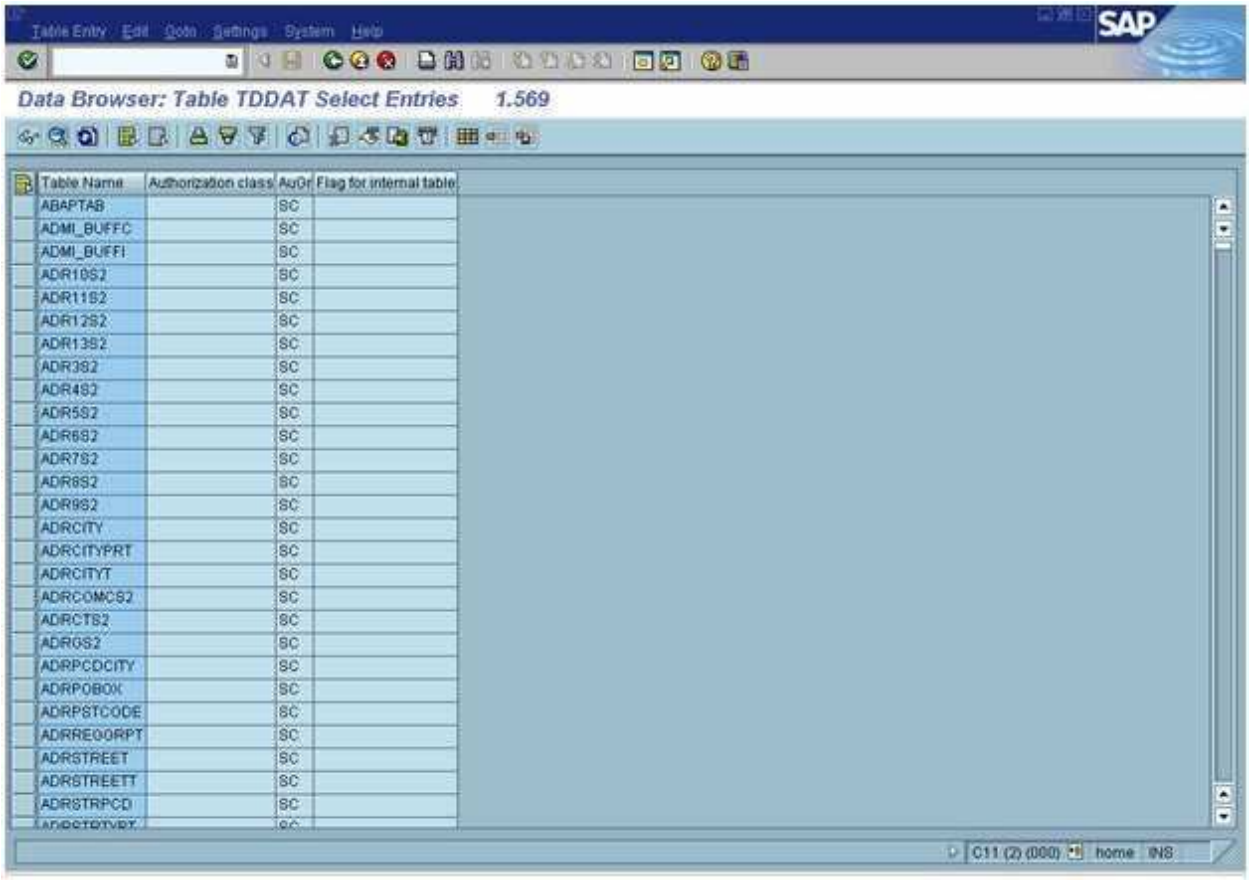
But when you want to execute USR40, it will give authorization error like "**you are not authorized to display this table**". Because you were not added the Auth Group for USR40.



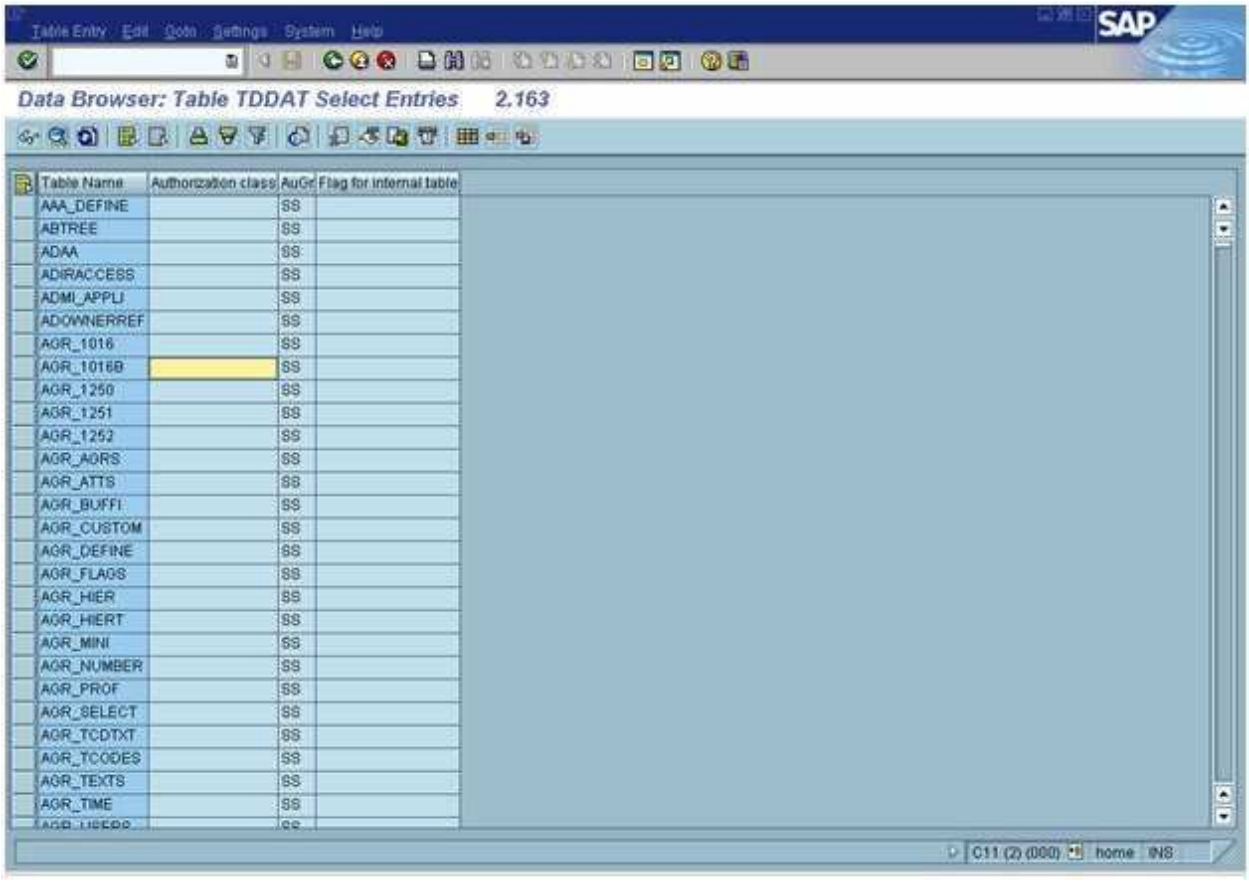
Causion:

When you ADD Auth Group to DICBERCLS it doesn't seem that you have only that table access, you can access all the table which has the same Auth Group maintained in TDDAT table.

In this example you can find, **there are 1569** tables, which has the same Auth Group (SC).



there are **2163** tables, which has the same Auth Group (SS).



So you can access all the table which is listed up.

Summary:

1. YOU can now find AUTH GROUP to a table,

2. You can now add AUTH GROUP to a **S_TABU_DIS** with your project requirements.

Problem of User Buffer !!!!!

Suppose, Two user **X** and **Y** both have Role **A** (**SU01D, SE16**). User **X** is able to run the **SU01D** but **Y** is not be able to Run the **SU01D**.

Please analyze the problem and what will be the solutions?

Let .

- There are no error record found in **ST01** for user Y.
- Only Role **A** has SU01D TCODE.

Problem Analysis:

- May be user comparison is not done properly for the user Y.
- You can refresh the User Buffer (Logoff and Login)

- No need to go to ST01 cause No record is there (as mentioned).
- It may be, User buffer can store maximum of **312** Profile, it may be possible user (**Y**) has more than 312 Profiles.

(why 312 Profiles: Because user buffer is String buffer which can hold maximum 3750 characters. And a profile contains 12 character, so an user can hold maximum 3750/12 ~ 312 profile.)

Solutions:

Please assign a reference User to user **Y**. And assigned Role **A** to the reference user, So **Y** can access Role **A**.

Please go through this link for assign the reference user to a Dialog user.

Note: **There are no limitation of Profile for Reference user.**

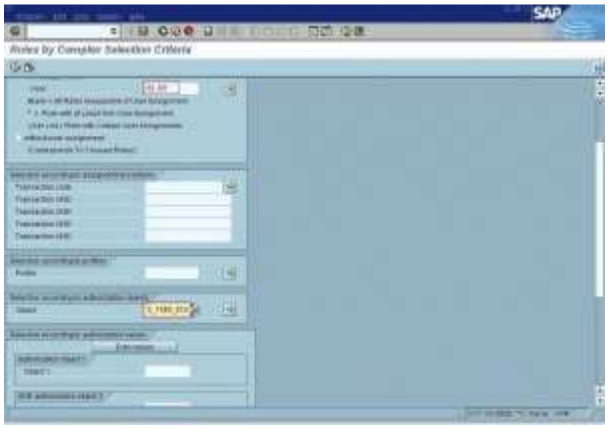
How to find, numbers of table an user can access?

- General,
- Important!!!,
- SAP Security Interview questions,
- SAP Security- Authorizition,
- Tac n Ticks

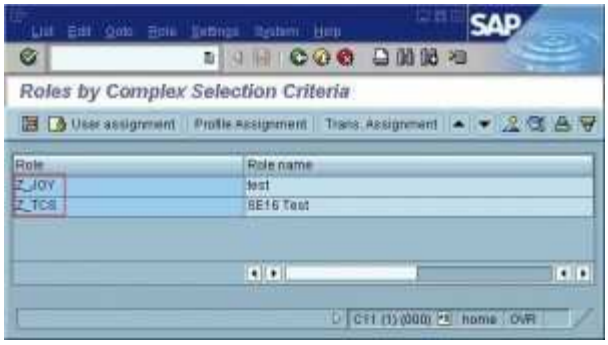
An User "BIJOY" is assigned some role in SAP. How to find, how many table the user can access in SAP, I got this question In SAP Security Facebook Page.

As we know table auth objects are S_TABU_DIS and S_TABU_CLI (this one is for cross client).

1. So at first we have to check which role contains those Authorization Objects.
Goto SUIM and ROLE -> "Roles by complex selection Criteria"
Select User as "BIJOY" and Authorization Object as S_TABU_DIS. You can select both Auth Objects.

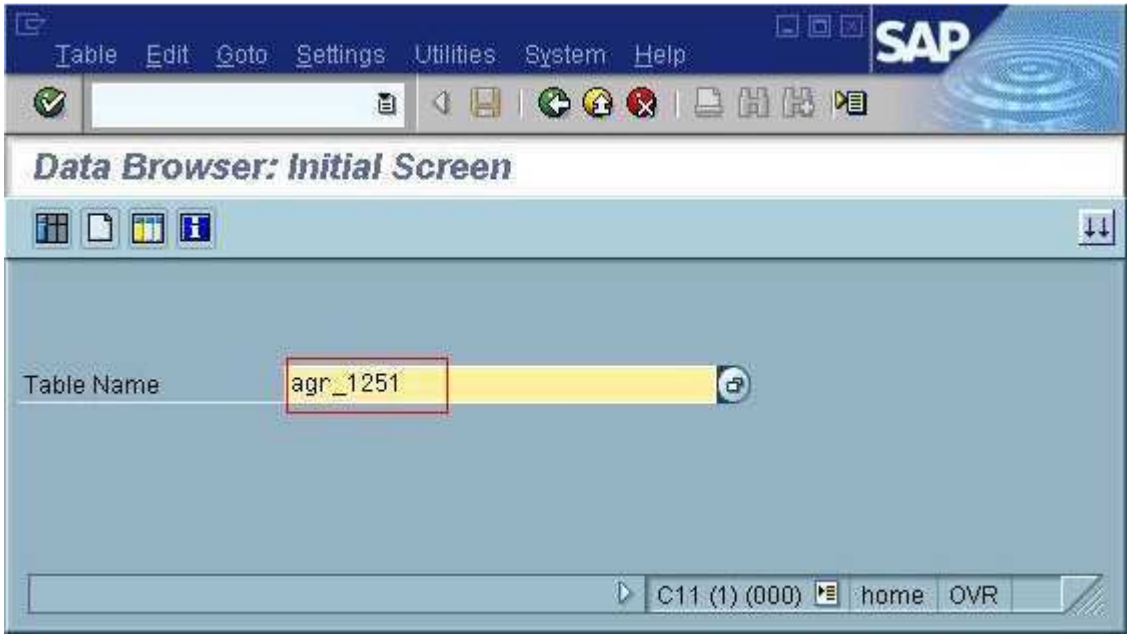


2. As I got,Roles **Z_JOY** and **Z_TCS** contains **S_TABU_DIS Authorization Object**.

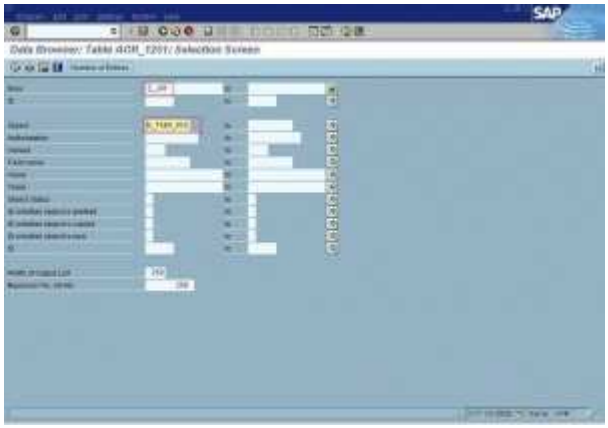


3. Now we have to find How many **Authorization Group** are present in those roles

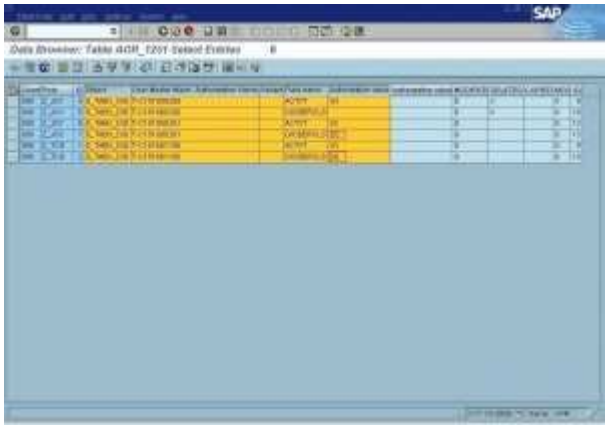
4. Goto **SE16** (Data Browser) -> **AGR_1251** (table)



5. Paste those roles **Z_JOY** and **Z_TCS** (from Step 1 and 2) and authorization as **S_TABU_DIS**.



6. Output is Like :

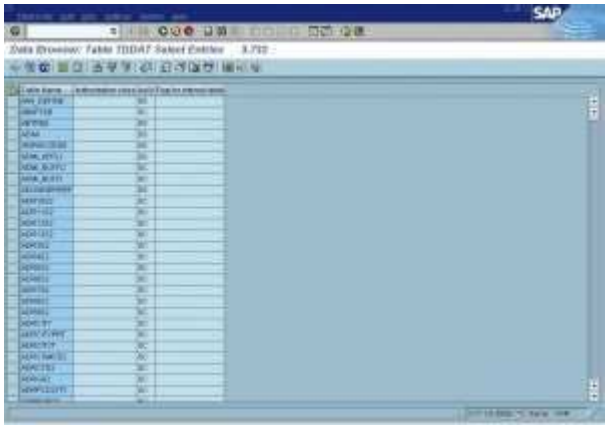


7. Here we got “SC” and “SS” Authorization Group. If the List is too long, just copy this into a **excel** file and filter the **Field Name** and select **DICBERCLS.** So you can get all authorization group.

8. Now we have to find how many tables are linked with those authorization Group.

9. Goto SE16 (Data browser) -> **TDDAT** (table). Select the authorion tab and paste all the authorization Group.

10. Final Output:



So, the user “BIJOY” can access 3732 table.

How to assign a Reference user to a Dialog user ?@!

- Important!!!,
- SAP Security Interview questions,
- Tac n Ticks

What is ‘reference’ user type in SU01? and when do you use it?

Reference user is when a user gets his authorizations from another user ID. This can be practical for internet users. You need to be careful about this type of access, as it will not show up in your ordinary SUIM0 reports! Or **AGR_USERS.**

Reference user is used only to assign additional authorizations. you can not login by using reference user

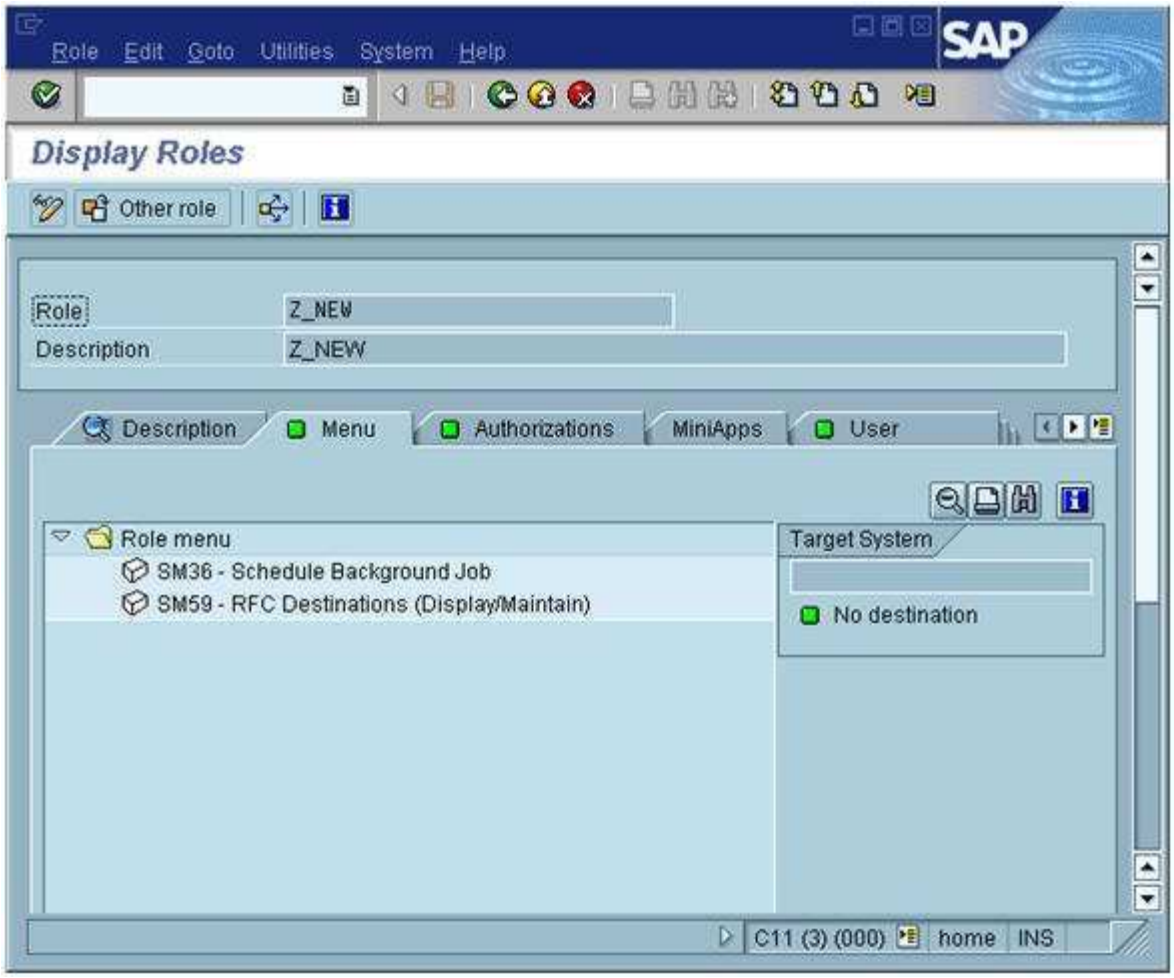
User type for general, non-person related users that allows the assignment of additional identical authorizations, such as for Internet users created with transactions SU01. You cannot log on to the system with a reference user.

To assign a reference user to a dialog user, specify it when maintaining the dialog user on the Roles tab page. In general, the application controls the assignment of reference users. This assignment is valid for all systems in a Central User Administration (CUA) landscape. If the assigned reference user does not exist in a CUA child system, the assignment is ignored.

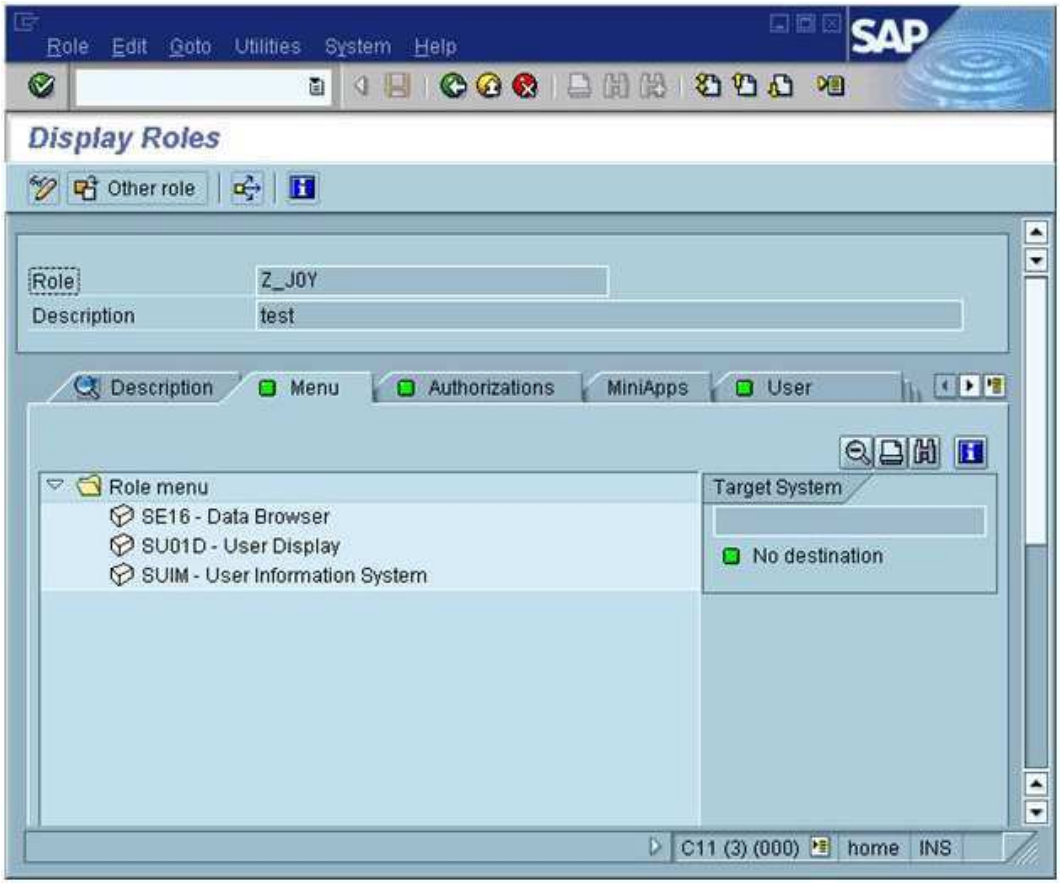
How to assign a Reference user to a dialog user.

suppose we have two roles Z_NEW and Z_TCS.

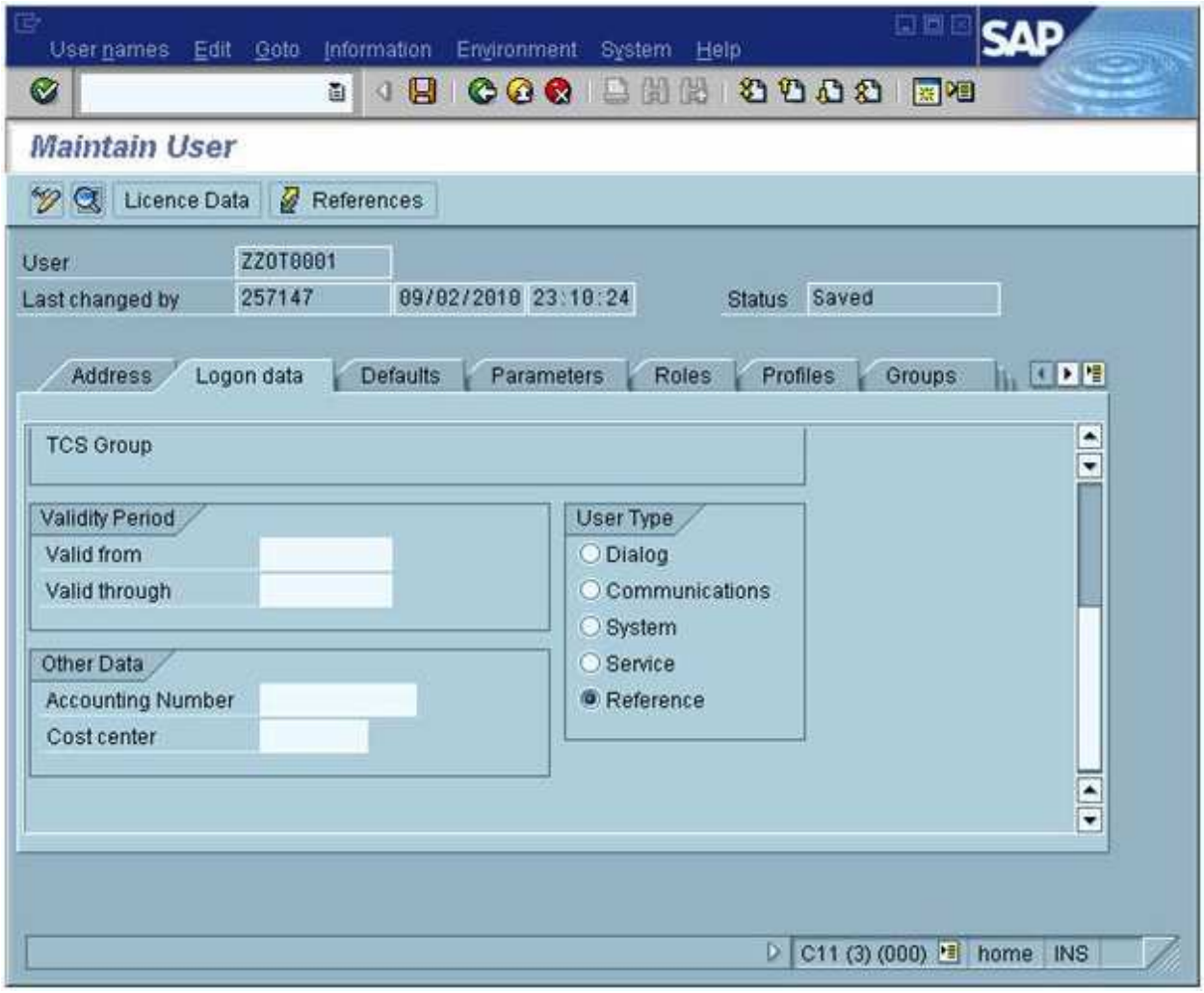
Z_NEW contains TCODE’s of SM36 and SM59.



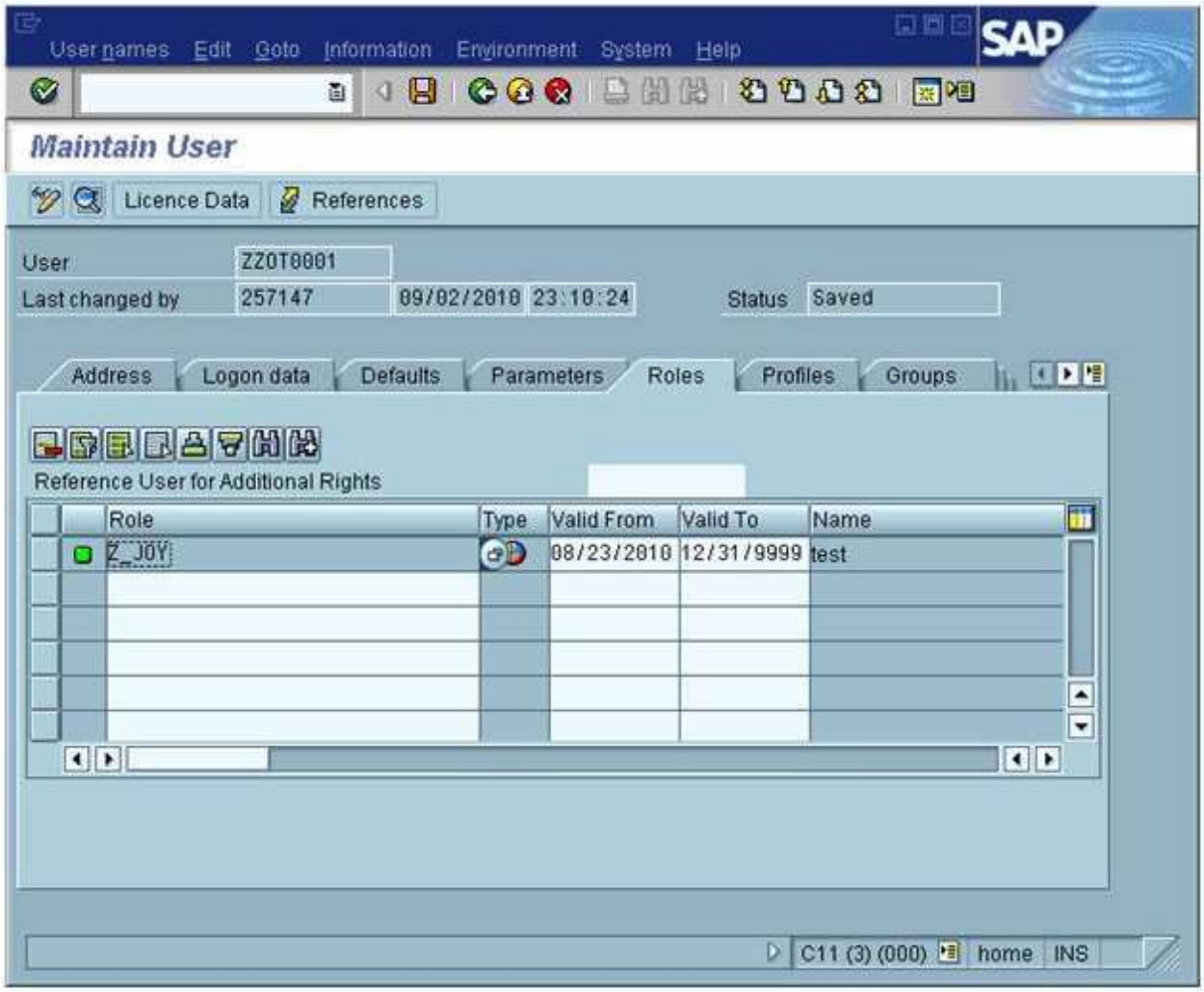
Z_JOY contains TCODE's of SE16, SU01D and SUIM.



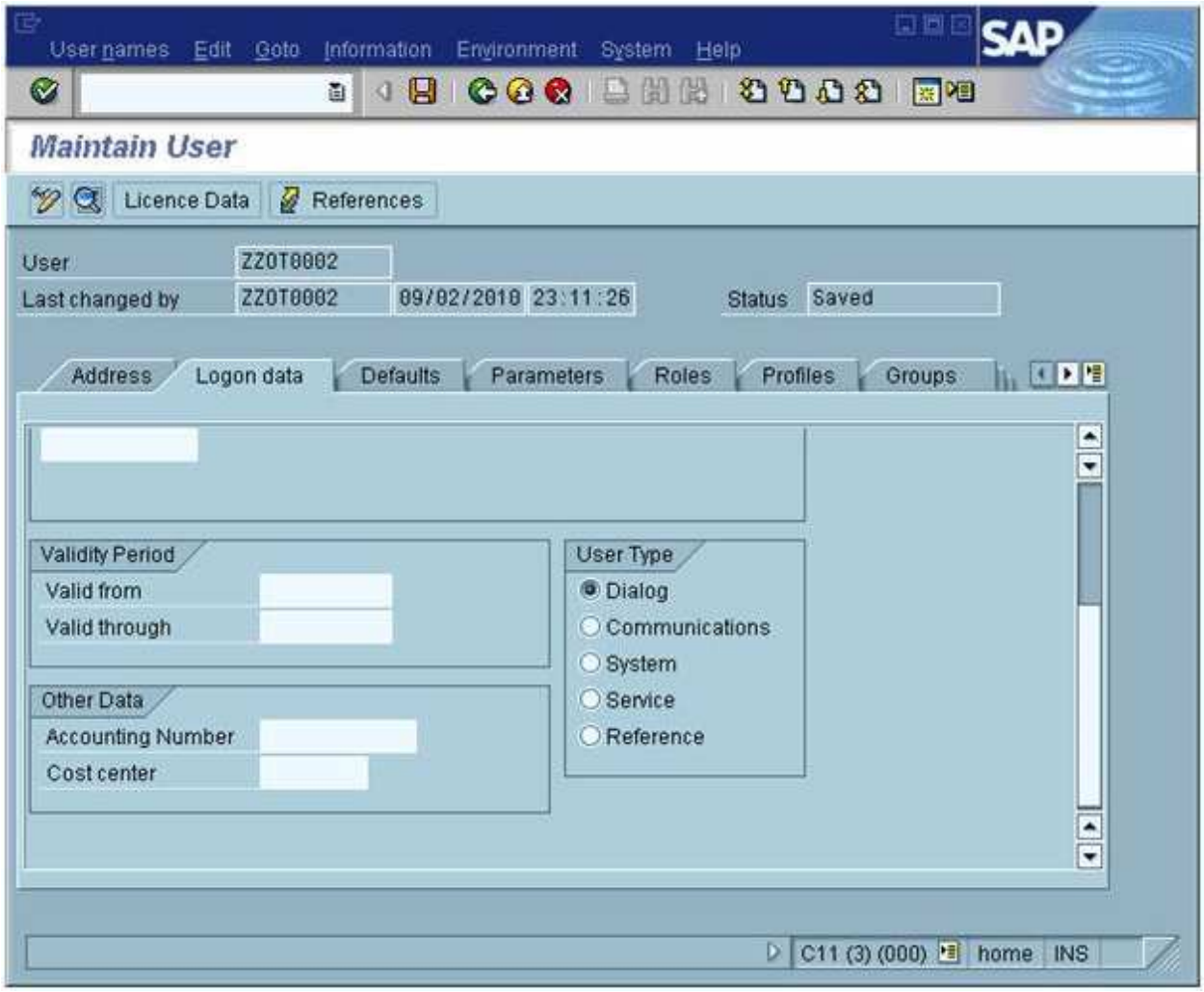
And we created a REFERENCE type user ZZOT0001.

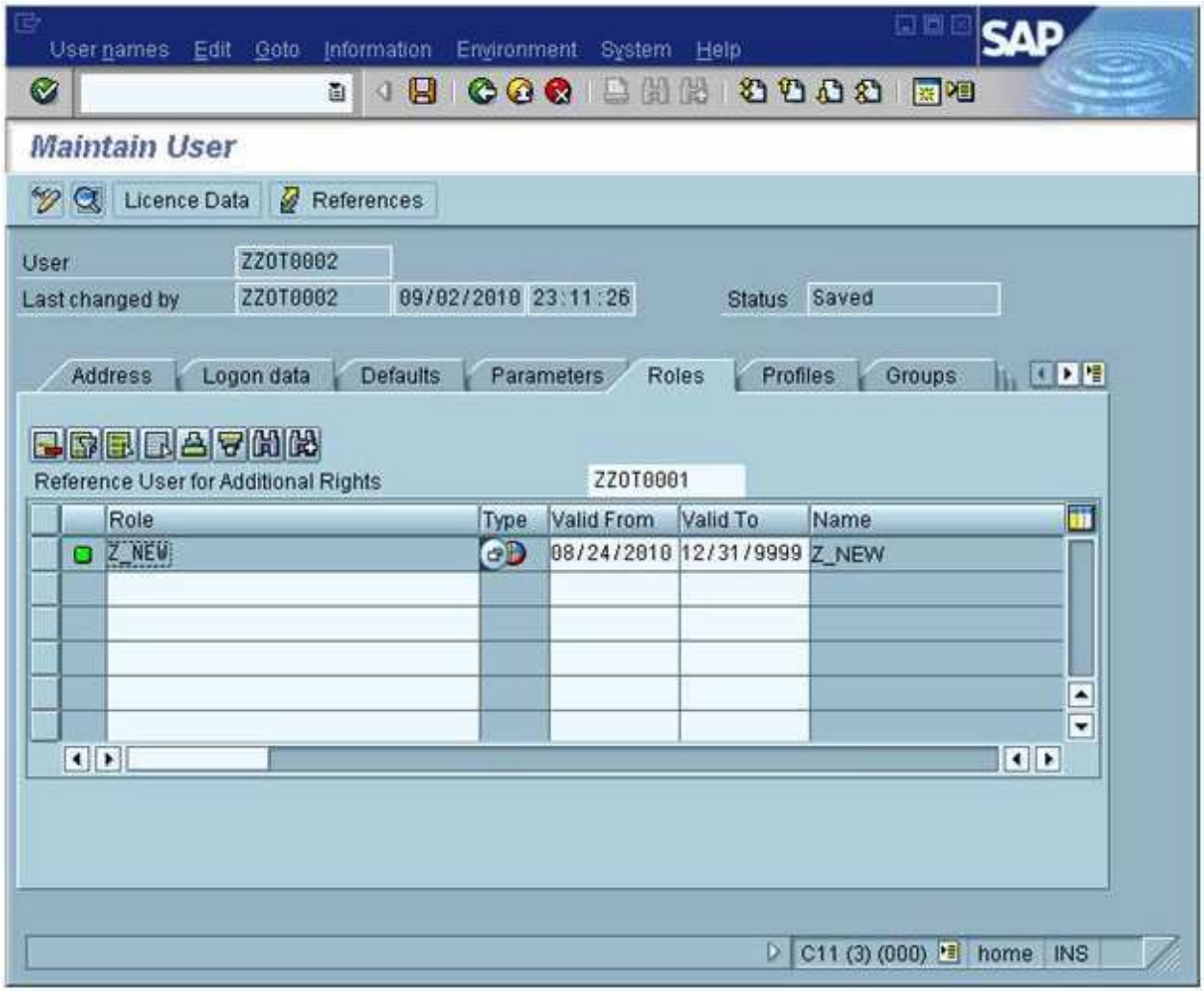


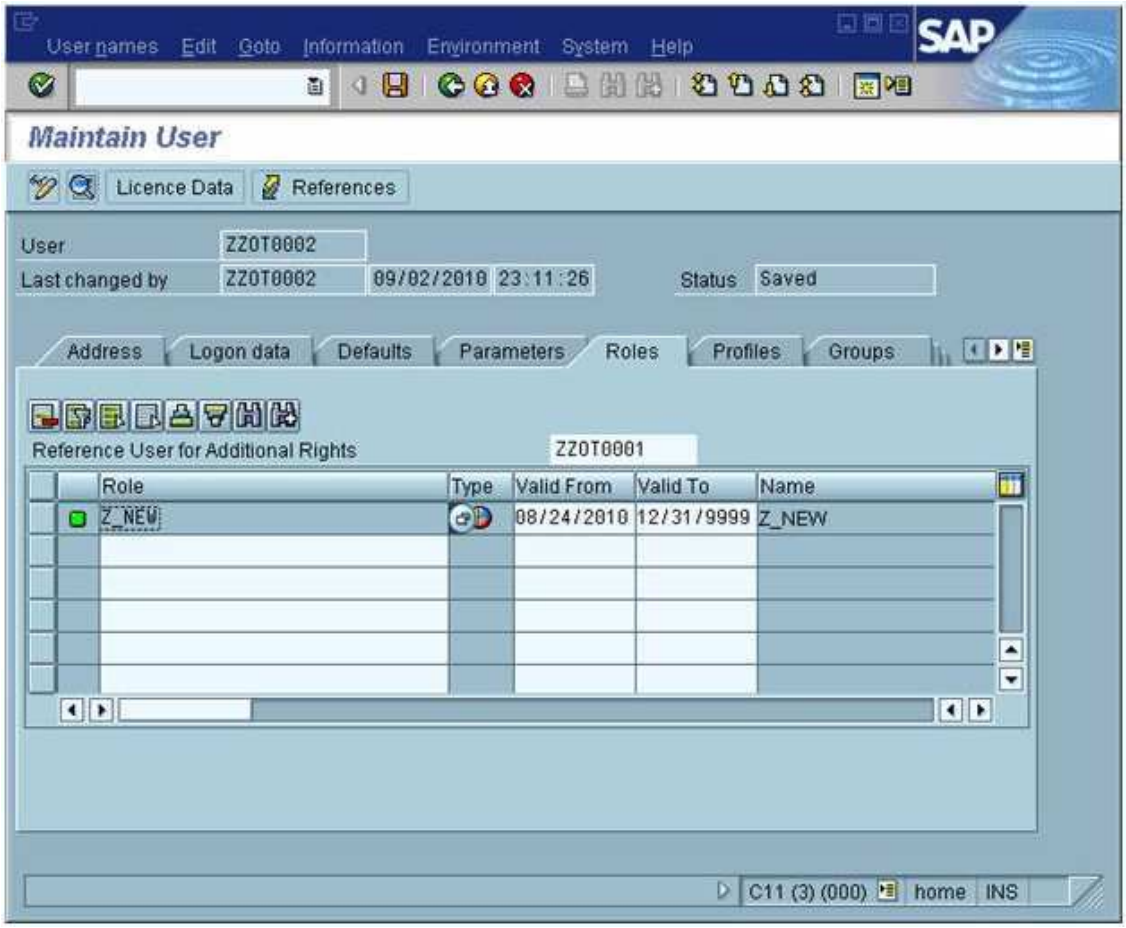
Which has Z_JOY Role (SE16, SU01D and SUIM).



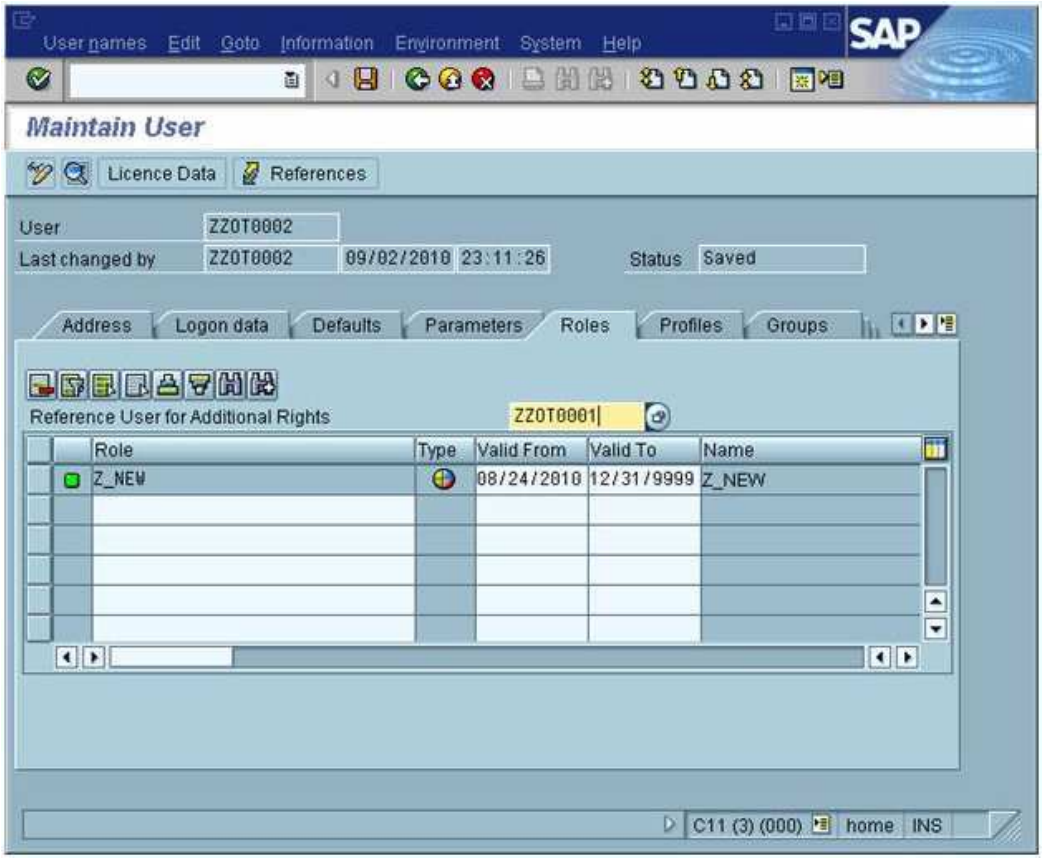
Now we create a new Dialog user ZZOT0002 and assign role Z_NEW to it.


User names Edit Goto Information Environment System Help
SAP
Maintain User
Licence Data
References
User
ZZOT0002
Last changed by
ZZOT0002
09/02/2010
23:11:26
Status
Saved
Address
Logon data
Defaults
Parameters
Roles
Profiles
Groups
Validity Period
Valid from
Valid through
User Type
Dialog
Communications
System
Service
Reference
Other Data
Accounting Number
Cost center
C11 (3) (000)
home
INS

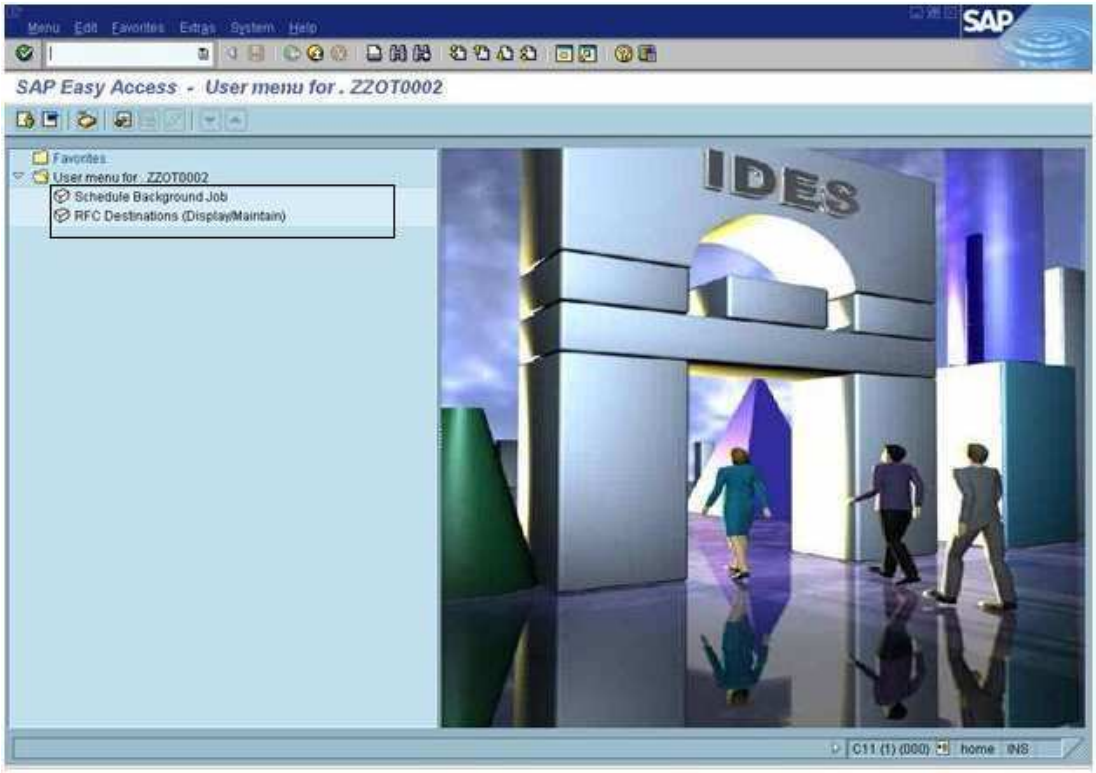

User names Edit Goto Information Environment System Help
SAP
Maintain User
Licence Data
References
User ZZOT0002
Last changed by ZZOT0002 09/02/2010 23:11:26
Status Saved
Address Logon data Defaults Parameters Roles Profiles Groups
Reference User for Additional Rights ZZOT0001
Role Type Valid From Valid To Name
Z_NEW 08/24/2010 12/31/9999 Z_NEW
C11 (3) (000) home INS



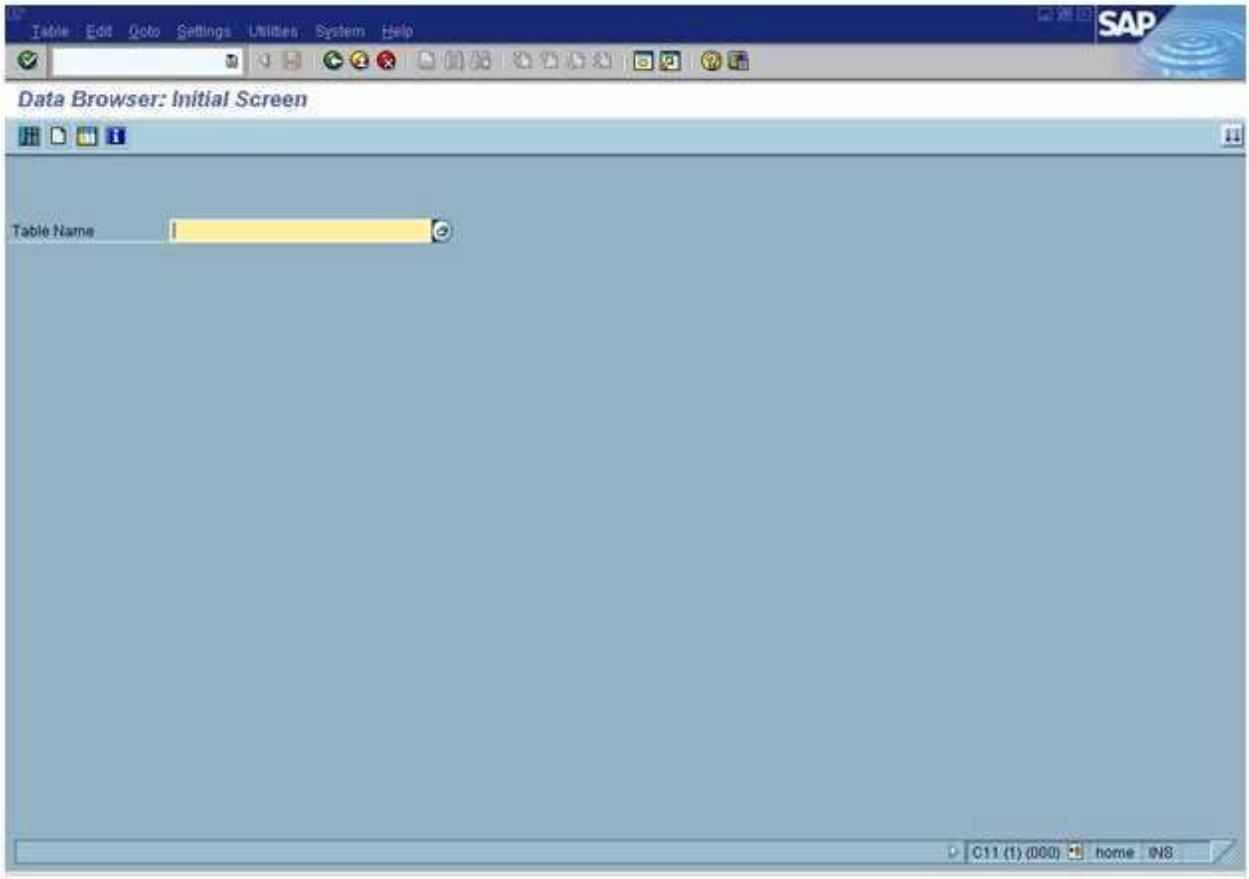
And assign the **REFERENCE user ZZOT0001** to “REF user for additional rights” field.



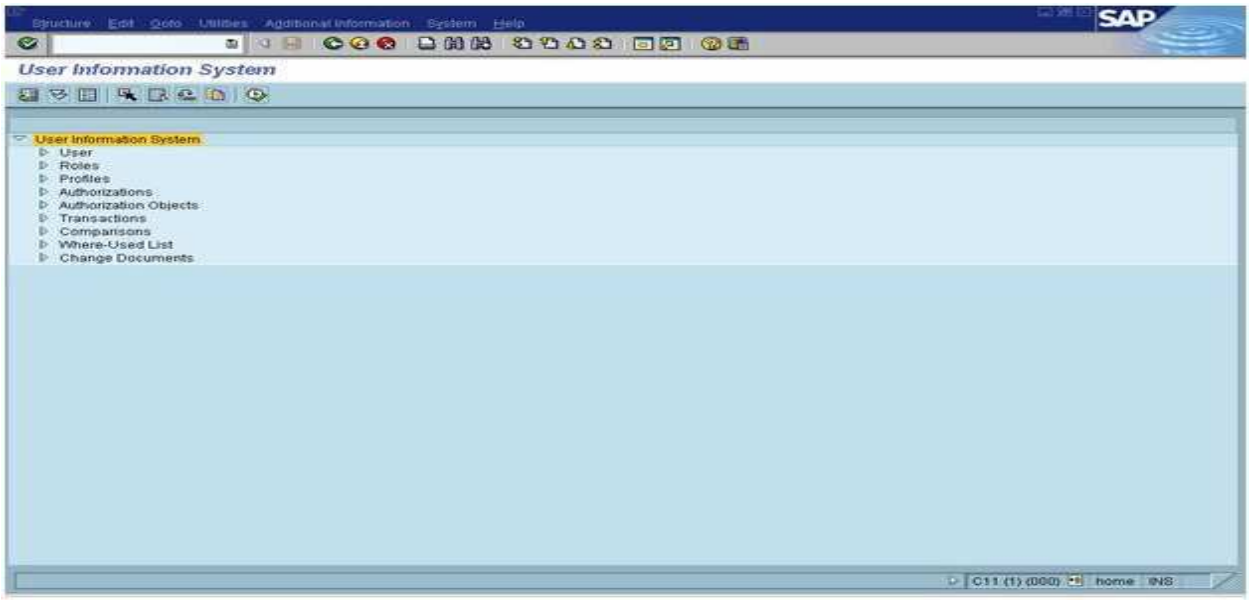
Now login through ZZOT0002 user it only shows **Z_NEW** roles. (SM36 and SM 59).



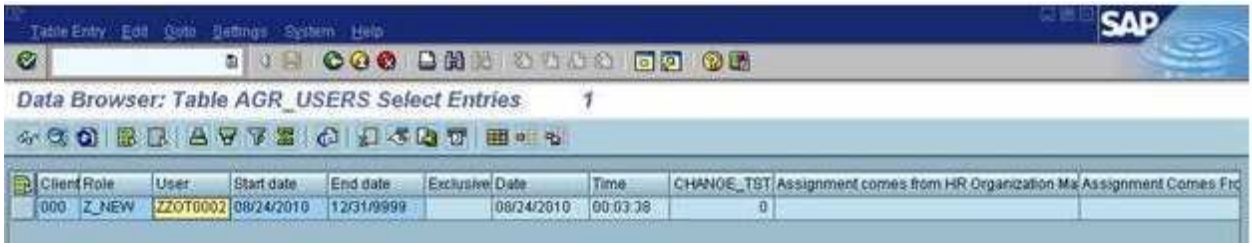
But when you execute **SE16** it will execute with **no authorization errors** .



And you will execute SUIM also.



But **Roles of reference user will never shows for the dialog users**. Here it shows only Z_NEW, not **Z_JOY**.



You should be very cautious when creating reference users.

- If you do not implement the reference user concept, you can deactivate this field in accordance with SAP Note 330067.
- We also recommend that you set the value for the Customizing switch REF_USER_CHECK in table **PRGN_CUST** to "E". This means that only users of type REFERENCE can then be assigned. Changing the Customizing switch affects only new assignments of reference users. Existing assignments are retained.
- We further recommend that **you place all reference users in one particularly secure user group to protect them from changes to assigned authorizations and deletion.**

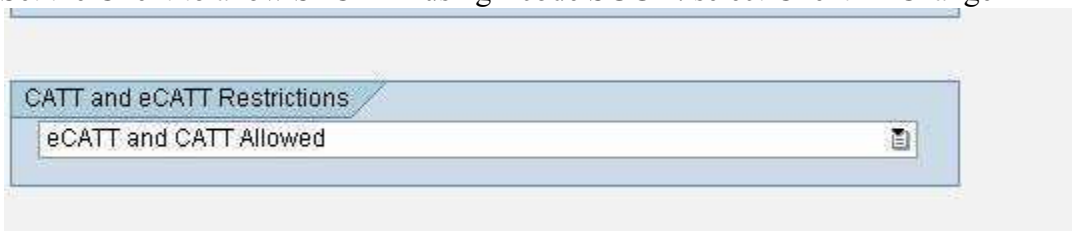
SECATT

What and Why SECATT ?

Computer Aided Test Tools (CATTs) are used within the context of SAP Best Practices to create master data and to automate technically oriented activities such as connectivity. For example, you can use CATTs to create master data in all components of the system landscape in which example data is
needed. Or you can use them to automatically carry out activities to create initial technical settings, such as RFC connections.
SECATT is an SAP Testing Tool used to automate & test business scenarios in R/3. Each test generates a detailed log that documents the test process and results. SECATT enables automatic testing in SAP GUI for Windows and SAP GUI for Java.

Enable SECATT:

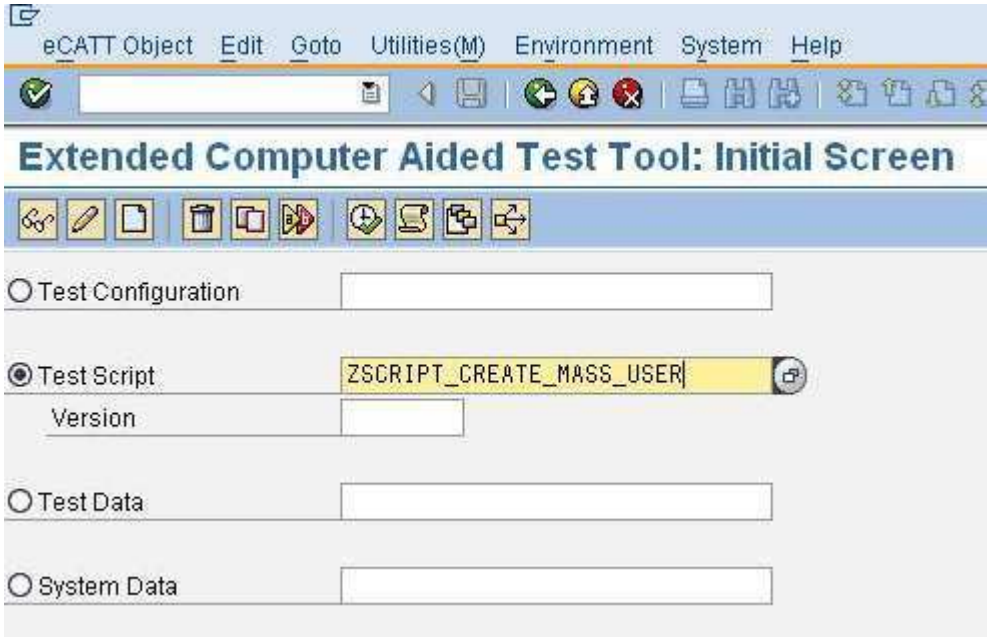
Set the Client to allow SECATT using Tcode **SCC4** : select Client -> Change



Create Mass users using SECATT

In every SAP Implementation / Installations one of the major activity is User Administration, which includes from user creation, setting initial password, security etc.
Suppose if there is a requirement of says more than 500 users ID creation! Imagine the efforts using **SU01.**
My objective is creating mass user short time with less administrative efforts.
The extended Computer Aided Test Tool (Tcode : SECATT) will help us accomplish our goal in very short time .

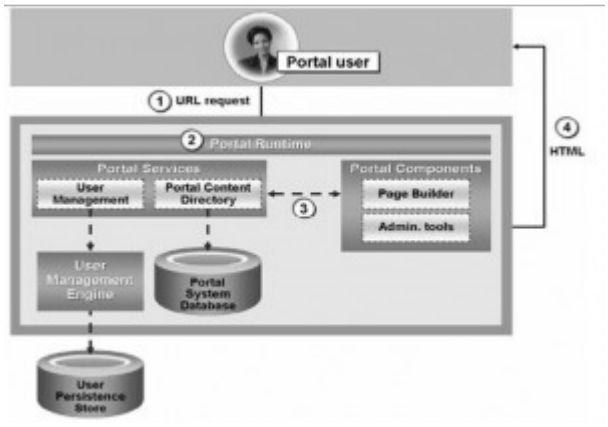
In short in our case SECATT is a set of Test Script & Test Configuration.
Test Script: A script contains one or more recorded transactions.
T**est Configuration (Enable SECATT):** A test configuration is a persistent data object with a set of references to a test script, although you can execute test scripts alone.
Create the Script which includes recording of the transaction:
1) Tcode – **SECATT** , create new script ZSCRIPT_CREATE_MASS_USER



SAP Portal (Extended)

- SAP EP Portal

Flow of Request



Flow of Request

- Client sends an HTTP or HTTPs request
- The Portal Runtime parses the request and identifies

    -
        -
        - The requested object from the PCD.
        - User related data
- Following information is obtained based on permissions for the requested object:
    -
        -
        - The portal component to be executed
        - A set of properties to be passed to the portal component
- HTML is returned to the browser.

Portal Content

Portal Content Directory (PCD):

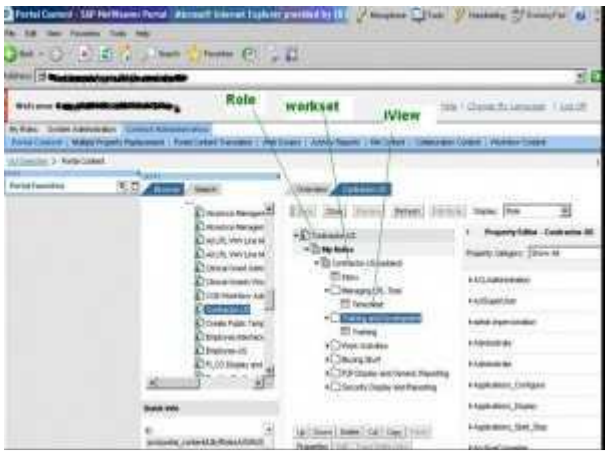
Important content objects are

- **iView** –Program that retrieves data from content sources and displays it in SAP content area.

- **Page** – consists of layout and assigned content.

- **Work set** – specific collection of tasks, services, and information that is part of a role.

- **Role** –Collection of tasks, services and information that is available for groups of users.



Portal Content

All Content objects are stored in a central persistence store, the Portal Content Directory (PCD) Provides the following functions:

- Delta links for reusing object instances

- Creation of relationships between objects

- Generic transport mechanism

- Personalization
- Object notification
- Versioning
- Filter mechanism and Search

Portal Content Studio

- Central environment for developing and managing the portal content.
- Use existing iView templates by supplying iView properties.
- Create simple portal pages by assigning existing content.
- To access the portal content studio, you must belong to the Content administrator.

Content Area

The following two areas appear in the content area:

- Portal Catalog:-

Displays content stored in the Portal Content Directory (PCD).Consists of the following areas:

- Portal catalog tab
- Portal content tree
- Quick info
- Editing Area:-

Consists of :

- Object tabs
- Object Editor Tools
- Object Editor
- Property Editor

Object Relations

Object properties:

- Parameters that permit the configuration and personalization of content.
- All objects have properties.
- Properties are object specific.
- Can be maintained with the property editor.

Delta Links

A delta link is a relationship between two objects in the PCD (Source and target objects).

- Source object passes its values to target objects.
- Changes made to source object are copied to the target object.
- Changes made to target object have no effect on the source object

Advantage:

- Objects can be reused or changed without changing the original object.
- **Methods of creating delta link:**
  - Use templates.
  - Copy and paste as delta link.
  - Insert in other objects as delta link.

Creating iViews

• Portal Content Studio provides a framework for creating iViews in a number of ways, without having to write any code.

• Content Administrator can create an iView using

• iView wizards

• Copies of existing iViews

• Once a new iView has been created, property editor is used to fine-tune some iView properties.

• Before assigning a new iView to the user, test the result with a preview.

- Typically iView is assigned to a page or a work set or role.

Web based URL iViews

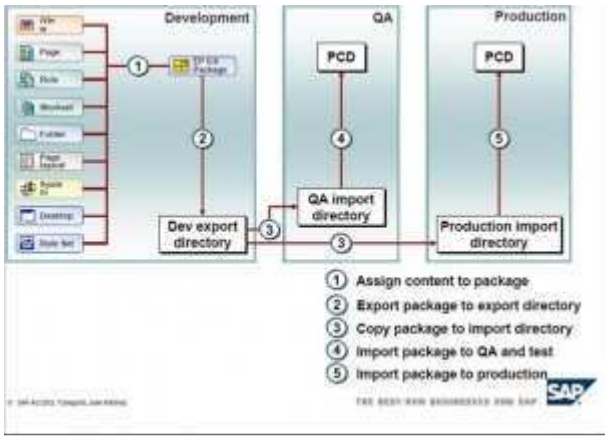
- iView that retrieves data directly from an internet of intranet site.
- Can designate selected parameters in the URL as variables.
- Specify the URL parameters using URL iview editor.
- Can be customized by content administrators and personalized at runtime by end users.

iView for SAP applications:

Following SAP applications are intergrated in SAP Enterprise portal as iViews.

- SAP transactions
- Internet Application components (IACs)
- Business Server Pages (BSP) applications
- WebDynpro applications
- SAP BW reports

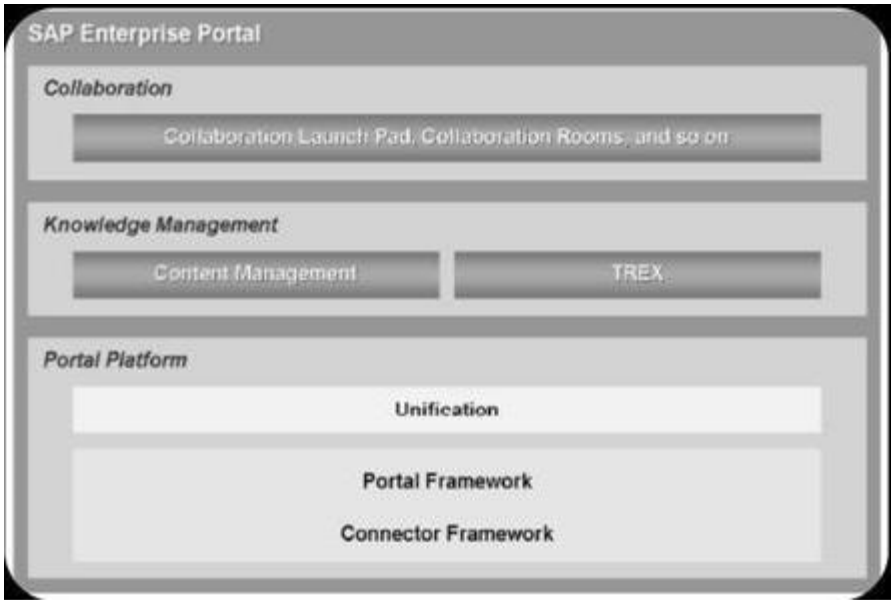
Flow of Portal Content through system landscape – Transports



Flow of Portal Content through system landscape – Transports

Blocks and Architecture of SAP Enterprise portal

- SAP EP Portal

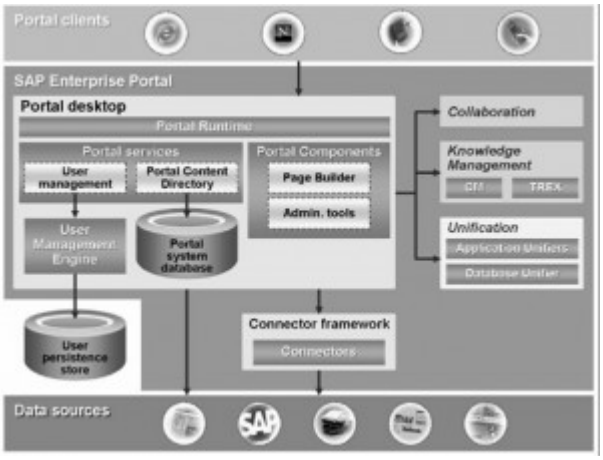


Blocks of EP

SAP Enterprise Portal Comprises three major building blocks:

- **Portal platform** - Has an open architecture that enables integration of SAP Net Weaver components such as knowledge management and collaboration. Components of portal platform:
  - Portal Desktop
  - Unification
  - Connector framework
- **Knowledge management** SAP Net Weaver component that offers a central, role-specific point of entry to unstructured information from various data sources in SAP EP. KM platform consists of :
  - Content Management (CM)
  - Search and Classification (TREX)
- **Collaboration** Collaboration with Net Weaver offers services that support communication and co-operation in enterprise specific business processes.

SAP Enterprise portal Architecture



portal architecture

- **Portal Runtime(PRT)** – Delivers the runtime environment for portal components and portal services.
- **Portal component** – Java code that is executed according to user requests and generates HTML output for display on the client.
- **Portal services** – Act as interfaces that are able to exchange procedures and data.(e.g) PCD service acts as an interface to the portal system database.

==========

Ref: www.help.sap.com

and special thanks to **Amrut**

3 comments

Feb
16

Characteristics and uses of SAP EP Portal

- SAP EP Portal

Characteristics of Portal?

- **Unification of Information from Different Systems**
  - Portal enables end users to get a single unified view of information gathered from different **BACKEND** systems
- **Targeted and Personalized information**
  - Portal provides mechanism where the information shown to the end user can be personalized based on their role
  - Personalization is possible at two levels
  - Portal Administrator level
  - User level
- **Single Sign On (SSO)**
  - Once users are authenticated by Portal, they get access to all the backend applications, if SSO is established between Portal and Backend applications
- **Easy & Multi-Device Accessibility**

- Portal Technology allows content to be accessible through multiple tools and devices such as Browser, Mobile Phones, PDAs etc

- **Content Management**
  - Portal allows Content Management capabilities
  - Extent and features vary from Portal to Portal
  - Some Portals actually integrate with different 3rd Party Specialized Content Management tools
- **Improved Organizational efficiency (process and transactional)**
  - Portal provides Organizational efficiencies both from process and transaction view
  - Imagine, if you have access to all the information you need on a single window, won't you work more efficiently?

Uses of Portal

Portals are actually applicable for different e-Business systems as mentioned below:

- B2E – Business to Employee Systems

  Eg. Your Organization Intranet probably is a Portal

- B2C – Business to Customer Systems

  Eg. Ebay.com, indiatimes.com

- B2B – Business to Business Systems

  Eg. SAP Service Market Place

The Portal system can bring together the proper information tailored to the type of user that the business wants to target.

==========

Reference : www.help.sap.com

And special thanks to **Amrut Koparde.**

Leave comment

Feb
15

What and Why EP Portal?

- SAP EP Portal

What is Enterprise Portal?

Specialized web-based interfaces that provide

- Single point of access to multiple backend applications
  - Single Sign On with Multiple Backend applications
- Single unified view of information and collaborative services
  - Portal aggregates all of the information in a way that is pleasing and relevant to the user regardless of where the information resides (which application) or in what format

Why Portal?

- Secure
- Role based Personalized Content
- Single Sign On with Multiple Backend applications
- Unification of information
- Collaborative Services
  -
    - Collaboration refers abstractly to all processes wherein people communicate and work together. Tools and Services, which enable this, are referred to as Collaborative Service.
    - Some of the Collaborative services, which may be offered by Portal, are
      - Document Sharing
      - Discussion Forums
      - Web Conferencing
      - Chat
    - These services offered may differ from vendor to vendor (Portal Product Vendor)

Portal aggregates all of the information in a way that is pleasing and relevant to the user regardless of where the information resides (which application) or in what format.

A Portal is	**A Portal is NOT**
• A single “place” or interface from which users can access multiple types of information organized around a common task or idea. • A place where users can complete self-directed tasks. • A “One Stop Shop” for information and transactions. • Easily usable by the intended audience without significant training or support. • A website that offers a single entry point to Enterprise Information, Applications and Processes and provide a way for Customers, Partners and Employees to access information and conduct Business. • A website that target specific audiences, providing collaboration, work-flow and community services in a	• A piece of Software or Product for sale. Rather software enables the Portal. • A website with just HTML pages, put together. Rather, it combines information, transactions, support and management / governance. • Necessarily expensive and complicated. • Specific or limited to one function. • Any web enabled version of a vendor’s product or application.

personalized manner.	

Will Post Other EP Doc shortly…..